2/2013

Datenschutz Nachrichten

36. Jahrgang
ISSN 0137-7767
9,00 Euro



Datenschutz mit Hindernissen

■ Outsourcing von Datenverarbeitung: Probleme der Funktionsübertragung ■ Google Glass, IT-Brillen und informationelle Selbstbestimmung ■ Meldepflicht von Datenschutzvorfällen – Anforderungen an das Datenschutzmanagement ■ BigBrotherAwards 2013 ■ Die Arroganz von Apple ■ Buchbesprechung ■ Nachrichten ■ Rechtsprechung ■

Deutsche Vereinigung für Datenschutz e.V.
www.datenschutzverein.de

Inhalt

Termine

Sonntag, 28. Juli 2013, 10:00 Uhr
DVD-Vorstandssitzung
Berlin. Anmeldung in der Geschäftsstelle
dvd@datenschutzverein.de

Donnerstag, 1. August 2013
Redaktionsschluss DANA 3/13
Thema: „Kommunale Software“

Mittwoch, 11. September 2013 bis
Samstag, 14. September 2013
14. Herbstakademie 2013
Law as a Service (LaaS) – Recht im Internet- und Cloud-Zeitalter
Humboldt Universität in Berlin
http://www.dsri.de/herbstakademie/herbstakademie.html

Montag, 16. September 2013 bis
Freitag, 20. September 2013
GI-Jahrestagung 2013
Koblenz
http://www.informatik2013.de

Samstag, 19. Oktober 2013
DVD-Vorstandssitzung
Bonn. Anmeldung in der Geschäftsstelle
dvd@datenschutzverein.de

Sonntag, 20. Oktober 2013
DVD-Mitgliederversammlung
Bonn.
dvd@datenschutzverein.de

DANA
Datenschutz Nachrichten
ISSN 0137-7767
36. Jahrgang, Heft 2

Herausgeber
Deutsche Vereinigung für Datenschutz e.V. (DVD)
DVD-Geschäftsstelle:
Rheingasse 8-10, 53113 Bonn
Tel. 0228-222498
Konto 1900 2187, BLZ 370 501 98, Sparkasse KölnBonn
E-Mail: dvd@datenschutzverein.de
www.datenschutzverein.de

Redaktion (ViSdP)
Sönke Hilbrans
c/o Deutsche Vereinigung für Datenschutz e.V. (DVD)
Rheingasse 8-10, 53113 Bonn
dvd@datenschutzverein.de
Den Inhalt namentlich gekennzeichneter Artikel verantworten die jeweiligen Autoren.

Layout und Satz
Frans Jozef Valenta, 53119 Bonn
valenta@t-online.de

Druck
Onlineprinters GmbH
Rudolf-Diesel-Straße 10
91413 Neustadt a. d. Aisch
www.diedruckerei.de
Tel. +49 (0)91 61 / 6 20 98 00
Fax +49 (0) 91 61 / 66 29 20

Bezugspreis
Einzelheft 9 Euro. Jahresabonnement 32 Euro (incl. Porto) für vier Hefte im Jahr. Für DVD-Mitglieder ist der Bezug kostenlos. Das Jahresabonnement kann zum 31. Dezember eines Jahres mit einer Kündigungsfrist von sechs Wochen gekündigt werden. Die Kündigung ist schriftlich an die DVD-Geschäftsstelle in Bonn zu richten.

Leserbriefe
Leserbriefe sind erwünscht. Deren Publikation sowie eventuelle Kürzungen bleiben vorbehalten.

Abbildungen, Fotos
Frans Jozef Valenta,
Seite 59: Fabian Kurz

Editorial

Liebe Leserinnen, liebe Leser,

lange hat der Sommer auf sich warten lassen. Und vergeblich warten mussten wir in diesem Frühjahr auch auf Durchbrüche beim Datenschutz. Damit meinen wir nicht die überfällige Beerdigung des Regierungsentwurfs zum Beschäftigtendatenschutz. Wir hätten uns aber etwa über schnelle Klarheit über die durch Tausende von Änderungsvorschlägen etwas unübersichtlich gewordene Weiterentwicklung des Entwurfs der EU-Datenschutz-Grundverordnung gefreut. Wir bekommen: ein Wahlkampfsommerloch und neue grausame Wahrheiten über die Datenkrake NSA. Datenschutz mit Hindernissen also. Es gibt auch welche, die Hindernisse anpacken: wir geben Ihnen einen kurzen Überblick über die diesjährigen Big-Brother-Awards (BBA), die wieder ausgesuchte Datenkraken an den Haken genommen haben. Außerdem dokumentieren wir ein sicher bald als „apple-Entscheidung“ bekannt werdendes Urteil des Landgerichts Berlin, - mit einem Kommentar von Rena Tangens. Gesetztes Wissen präsentieren wir Ihnen mit dem Beitrag von Prof. Anne Riechert, welche ein kritisches Resümee zum Konzept der Funktionsübertragung im Datenschutzrecht zieht. Karsten Neumann unterzieht die noch relativ junge Regelung zur Breach Notification einer faktengestützten Würdigung. Thilo Weichert schließlich bring uns auf den neuesten Stand bei Google Glass. Und natürlich wieder Nachrichten, Nachrichten, Nachrichten.

Anregende Lektüre und einen guten Start in den Sommer wünscht Ihnen

Sönke Hilbrans

Autorinnen und Autoren dieser Ausgabe:

Karsten Neumann
Vorstandsmitglied der DVD, Landesbeauftragter für Datenschutz Mecklenburg-Vorpommern a.D., Associate Partner der 2B Advice GmbH,
neumann@datenschutzverein.de

Anne Riechert
Professur für Datenschutzrecht und Recht in der Informationsverarbeitung an der Fachhochschule Frankfurt am Main.
Während ihrer Tätigkeit als Rechtsanwältin hat sie Unternehmen unter anderem in vertrags- und datenschutzrechtlichen Angelegenheiten beraten.
anne.riechert@gmx.de

Rena Tangens
Mitbegründerin und Vorsitzende des Bielefelder Vereins digitalcourage (ehemals FoeBuD), Mitglied der Jury bei den BigBrotherAwards.
rena.tangens@digitalcourage.de

Dr. Thilo Weichert
Leiter des Unabhängigen Landeszentrums für Datenschutz Schleswig Holstein, Kiel,
weichert@datenschutzzentrum.de

Anne Riechert

Outsourcing von Datenverarbeitung: Probleme der Funktionsübertragung

I .Einleitung

Das Konzept der Funktionsübertragung beruht auf der Annahme, dass Unternehmen Aufgaben, die die Verarbeitung von Kunden-oder Mitarbeiterdaten zum Gegenstand haben, vollständig auslagern dürfen. Die Frage ist nur: Warum? Denn zu berücksichtigen ist, dass keine datenschutzrechtliche Vorschrift eine solche Übertragung von Funktionen ausdrücklich regelt. Die Zulässigkeit wird vielmehr daraus hergeleitet, dass eine Norm des Bundesdatenschutzgesetzes die Übermittlung von Daten grundsätzlich erlaubt, *wenn kein Grund zur Annahme besteht, dass schutzwürdige Interessen der Betroffen überwiegen*. Da diese Abwägung jedoch ohne Mitspracherecht der Betroffenen allein in die Hände der Unternehmer gelegt wird, können letztere das Verbotsprinzip mit Erlaubnisvorbehalt (§ 4 Abs. 1 BDSG) mühelos in ihrem Sinne anwenden. Diese Maxime des Datenschutzrechts fordert für jede Erhebung, Verarbeitung oder Nutzung von Daten eine gesetzliche Erlaubnis oder die Einwilligung der Betroffenen. Für die Verwirklichung des gesetzgeberischen Ziels, das Persönlichkeitsrecht des Einzelnen zu schützen, ist es allerdings mehr als fraglich, ob der Gesetzgeber eine solche Vorgehensweise tatsächlich als interessengerecht einstufen kann. Es ist selbstredend, dass der Fokus nicht auf das Bedürfnis der Unternehmer nach bequemer und pragmatischer Gestaltung von Geschäftsprozessen gerichtet sein darf, welches zu dem Datenschutzinteresse der Betroffenen völlig konträr ist. Unternehmen haben keinen Anspruch darauf, in unkomplizierter Weise an den Vorteilen einer arbeitsteiligen Wirtschaft teilzuhaben.[1] Aber die Betroffenen haben ein grundgesetzlich garantiertes Recht auf informationelle Selbstbestimmung.

Ein weiteres Outsourcing-Konzept, die Auftragsdatenverarbeitung gemäß § 11 BDSG, schützt zwar die Interessen der Betroffenen, ist jedoch für die Unternehmer in der praktischen Durchführung weniger angenehm, da diese die Beachtung enger gesetzlicher Anforderungen erfordert und lediglich für die Auslagerung von unterstützenden Tätigkeiten in Betracht kommen soll. In den folgenden Ausführungen werden diese beiden Outsourcing-Konzepte der Funktionsübertragung und der Auftragsdatenverarbeitung sowie ebenso eine vermittelnde Auffassung (Vertragstheorie) erörtert.

II. Merkmale der Auftragsdatenverarbeitung und der Funktionsübertragung

Auftragsdatenverarbeitung ist an die engen gesetzlichen Voraussetzungen des § 11 BDSG geknüpft und wird als weisungsgebundene Tätigkeit des Auftragnehmers (Dienstleisters) verstanden. Es wird stets darauf verwiesen, dass bei einer Auftragsdatenverarbeitung der Auftraggeber „Herr der Daten“ bleibt, der Auftragnehmer nur als „verlängerter Arm“ und „ausgelagerte Abteilung“ fungiert.[2] In diesem Sinne hat der Auftragsdatenverarbeiter lediglich eine unterstützende Funktion für den Auftraggeber inne.[3] Ein wichtiges Kriterium ist die Eingliederung des Auftragsdatenverarbeiters in das Unternehmen der auftraggebenden Stelle. Beide stellen aus rechtlicher Sicht eine Einheit dar und der Auftragnehmer ist an die Vorgaben des Auftraggebers gebunden.[4] Derjenige hingegen, der in Funktionsübertragung tätig ist, ist selbstständig für die Rechtmäßigkeit der Datenverarbeitung und die Wahrung der Betroffenenrechte verantwortlich.[5] Er darf die Aufgabe, die vollständig auf ihn übertragen bzw. ausgelagert ist, somit eigenverantwortlich durchführen und ihm obliegt die rechtliche Zuständigkeit.[6] Die Einzelheiten der Abgrenzung sind streitig - sogar im Hinblick auf die identische inhaltliche Aufgabe. Letzteres ist vornehmlich von den unterschiedlichen Interessen abhängig, die einerseits wirtschaftlich und andererseits datenschutzrechtlich geprägt sind. So wird die Auslagerung der Personalverwaltung teilweise als Auftragsdatenverarbeitung[7] und teilweise als Funktionsübertragung eingestuft.[8] Der Arbeitsbericht der ad-hoc-Arbeitsgruppe „Konzerninterner Datentransfer“ des Regierungspräsidium Darmstadt macht diese Streitfrage zwischen Aufsichtsbehörden und Wirtschaftsvertretern besonders deutlich[9]: „Zwar besteht Einigkeit darüber, dass eine Auftragsdatenverarbeitung bei Vorgabe eines ausdifferenzierten Entscheidungsbaums zur Aufgabenerfüllung in Betracht kommt, da in diesem Falle dem Auftragnehmer keinerlei inhaltlicher Ermessenspielraum überlassen bleibt“.[10] Streitig sei hingegen zwischen den Aufsichtsbehörden und den Wirtschaftsvertreten, inwieweit das Kriterium der fehlenden Entscheidungsbefugnis des Dienstleisters relevant sei bzw. welche konkrete Bedeutung es habe.[11] In dem Arbeitsbericht wird in diesem Zusammenhang ebenso darauf verwiesen, dass Vertreter der Wirtschaft die Auslegung der Auffassung der Aufsichtsbehörden für zu eng hielten, die darauf abziele, dass Auftragsdatenverarbeitung dann ausscheiden müsse, wenn der Auftragsdatenverarbeiter auch nur den kleinsten Ermessenspielraum habe.[12] Primär geht es also ebenso um die Frage, inwieweit Unternehmer sich eine Wahl- und Interpretationsfreiheit hinsichtlich Auftragsdatenverarbeitung und Funktionsübertragung herausnehmen.

III.Vergleich der Anforderungen

1. Auftragsdatenverarbeitung

Die Möglichkeit, Daten im Auftrag

verarbeiten zu lassen, ist –wie oben dargestellt- an enge gesetzliche Vorgaben geknüpft. Der Begründung zum Gesetzentwurf der Bundesregierung lässt sich entnehmen,[13] dass § 11 BDSG im Zuge der BDSG-Novelle II 2009 aus dem Grunde konkreter gefasst worden ist, da den nicht-öffentlichen Stellen oftmals nicht bekannt war, welche technischen und organisatorischen Maßnahmen von ihnen verlangt werden: Verträge zur Auftragsdatenverarbeitung wurden entweder nicht im Sinne des § 11 BDSG oder nicht schriftlich verfasst und ebenso selten Regelungen zur Löschung der Daten bzw. deren Rückgabe nach Erledigung des Auftrages getroffen.[14] Dementsprechend wurde die Möglichkeit einer Bußgeldahndung begrüßt, die nun in § 43 Abs. 1 Nr. 2b BDSG geregelt ist.[15] Auch die gesetzliche Verpflichtung zur Dokumentation des Kontrollergebnisses seitens der Auftraggeber stellt insgesamt einen wichtigen Faktor dar, da sich dieser ansonsten „nur in sehr zurückhaltender Weise von der Ordnungsmäßigkeit der Geschäftstätigkeit des Vertragspartners überzeugen“ werde.[16]

2.Funktionsübertragung

Die Funktionsübertragung findet keine ausdrückliche gesetzliche Grundlage. Ihre Rechtfertigung wird regelmäßig aus § 28 Abs. 1 S. 1 Nr. 2 BDSG hergeleitet.[17] Gemäß dieser Regelung ist eine Datenübermittlung zulässig, d.h. eine Weitergabe von personenbezogenen Daten an Dritte gemäß § 3 Abs. 4 Nr. 3 BDSG, *„soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt.“*

Aus datenschutzrechtlicher Sicht sind vornehmlich zwei Fragestellungen zu beantworten:

Erstens: Warum sollte § 28 Abs. 1 S. 1 Nr. 2 BDSG anwendbar sein?

Zweitens: Werden die schutzwürdigen Interessen der Betroffenen ausreichend berücksichtigt?

a. Anwendbarkeit von § 28 Abs. 1 S. 1 Nr. 2 BDSG?

Diesbezüglich ist zunächst streitig, ob die Alternative des § 28 Abs. 1 S. 1 Nr. 1 BDSG im Vordergrund steht und die ergänzenden Tatbestände Nr. 2 und Nr. 3 lediglich außerhalb von Schuldverhältnissen als Auffangklauseln zur Anwendung gelangen können.[18] Damit wäre die Frage der Zulässigkeit sehr zügig zu beantworten, da in den wenigsten Fällen eine Funktionsübertragung im Sinne von § 28 Abs. 1 S. 1 Nr. 1 BDSG tatsächlich erforderlich wäre.[19] Aber selbst die juristische Auffassung, die eine Wahlfreiheit zwischen den Alternativen des § 28 Abs. 1 BDSG unterstellt, verweist darauf, dass die verantwortliche Stelle den Anknüpfungspunkt weder beliebig auswählen noch kumulativ auf die Zulässigkeitsgründe zurückgreifen könne.[20] Es sei eine restriktive Auslegung im Sinne einer nur ausnahmsweise zulässigen Verarbeitung geboten.[21] Mit dieser einschränkenden Betrachtung ist ebenso verbunden, dass innerhalb der verantwortlichen Stelle nicht jedermann auf die Daten zugreifen oder diese frei verwenden darf.[22] Bei konsequenter Anwendung müsste auch diese zweite Ansicht aus Gründen des „erst-recht-Schlusses“ zu einer Ablehnung der Funktionsübertragung anhand des § 28 Abs. 1 S.1 Nr. 2 BDSG kommen, welche sie jedoch insgesamt für zulässig erachtet:[23] Wenn die Daten schon innerhalb der verantwortlichen Stelle nicht uneingeschränkten Nutzungsrechten unterliegen, dürften die Daten „erst recht“ nicht uneingeschränkt an Dritte gelangen. Dies führt zu der Frage, ob die personenbezogenen Daten tatsächlich die verantwortliche Stelle veranlassen dürfen ohne die Schutzmaßnahmen des § 9 BDSG kontrolliert und dokumentiert sicherzustellen, vor allem mit der grundsätzlichen Möglichkeit einer Zweckänderung durch die Dritten?[24] Die Regelung des § 28 Abs. 1 S. 1 Nr. 2 BDSG enthält dazu (anders als die Auftragsdatenverarbeitung) keine konkreten Anforderungen, sondern überlässt auch dies der Einschätzung des Unternehmers. Die schutzwürdigen Interessen der Betroffenen sind gerade nicht und unter Bußgeldandrohung unabdingbar mit einer schriftlichen Dokumentations- und Kontrollpflicht des Unternehmers verknüpft. Zudem: Wenn der Grundsatz der restriktiven und nur ausnahmsweise zulässigen Datenverarbeitung ernst genommen wird, müsste sich jeder Unternehmer stets zuerst die Frage stellen, ob ein Outsourcing tatsächlich zur Vertragsdurchführung erforderlich ist oder ob die Datenverarbeitung nicht ebenso intern stattfinden könnte. Eine solche Erforderlichkeit im Sinne des § 28 Abs. 1 S. 1 Nr. 1 BDSG lässt sich beim Outsourcing von Daten allenfalls unterstellen, wenn die Daten **konzernintern** verarbeitet werden **müssen**,[25] aber nicht für eine herkömmliche Unternehmer-/Kundenbeziehung. Hier ist eine externe Datenverarbeitung gemäß § 28 Abs. 1 S. 1 Nr. 1 BDSG nicht notwendig und eine kumulative Anwendung des § 28 Abs. 1 S. 1 Nr. 2 BDSG wäre (auch im Sinne der oben zitierten Meinung) einer kritischen Überprüfung zu unterziehen: Jedwede nur ausnahmsweise zulässige Datenverarbeitung erfordert besondere Prüfpflichten! Daher kann durchaus die Forderung aufgestellt werden, dass einem Unternehmer Funktionsübertragung dann verwehrt sein muss, wenn anhand objektiv zu bemessender Kriterien nicht feststellbar ist, dass ihm die eigenverantwortliche Datenverarbeitung – beispielsweise im Wege einer Auftragsdatenverarbeitung – unmöglich ist. Allein der Umstand eines kostengünstigeren Angebots genügt den Anforderungen des § 28 BDSG allerdings nicht.[26] Wenn außerdem vertreten wird, dass der Weg über § 28 Abs. 1 S. 1 Nr. 2 BDSG der verantwortlichen Stelle so lange versperrt bleiben muss, wie diese ihr Informationsziel anders erreichen kann,[27] muss eine solche Einschränkung ebenso für das „Wie“ der Datenverarbeitung gelten.[28] Letztendlich spielen bei diesem Punkt die im nachfolgenden behandelten schutzwürdigen Interessen des Betroffenen eine maßgebliche Rolle. Diese sind jedoch aufgrund der mangelnden gesetzlichen Vorgaben im Rahmen von § 28 Abs. 1 S. 1 Nr. 2 BDSG einer gewissen Beliebigkeit ausgesetzt.

b. Schutzwürdige Interessen der Betroffenen

Nachteilig an der Regelung des § 28 Abs. 1 S. 1 Nr. 2 BDSG ist insgesamt, dass der Gesetzgeber weder die „berechtigten Interessen“, die „schutzwürdigen Interessen“ noch die Anforderungen an die Abwägung zwischen diesen widerstreitenden Interessen definiert hat.[29] Unternehmen, welche die personenbe-

zogenen Daten ihrer Kunden oder Mitarbeiter outsourcen, können die wirtschaftliche Effizienz und ungehinderte Ausgestaltung ihrer Geschäftsprozesse prinzipiell höher ansiedeln als die Interessen der Betroffenen, da eine summarische Prüfung der jeweiligen Interessen durch den Unternehmer als ausreichend angesehen wird.[30] Aber müssen die Betroffenen nicht umgekehrt darauf vertrauen dürfen, dass ihre persönlichen Daten in der rechtlichen Verantwortung des konkreten Unternehmens – ihrem jeweiligen Vertragspartner – verbleiben? An dieser Stelle kann die Abwägung folglich ebenso ergeben, dass die schutzwürdigen Belange der Betroffenen einer Funktionsübertragung, nämlich der Weitergabe ihrer Daten an für Sie unbekannte Dritte grundsätzlich immer entgegenstehen.[31] Für diesen Fall ist entweder eine Einwilligung der Betroffenen gemäß § 4a BDSG oder die Auftragsdatenverarbeitung gemäß § 11 BDSG vorgesehen – wobei letztere eine Datenweitergabe lediglich unter der Voraussetzung zulässt, dass der (für die Betroffenen unbekannte) Empfänger weisungsgebunden ist und kontrolliert wird. Der Schutz des Persönlichkeitsrechts erfordert hier eine restriktive Betrachtung, vor allem wegen der weitreichenden Möglichkeiten der Zweckänderung gemäß § 28 Abs. 2 Nr. 1 BDSG sowie § 28 Abs. 5 BDSG. Diese führen zu dem untragbaren Ergebnis, dass der Dritte die personenbezogenen Daten gleichermaßen für seine eigenen und vor allem anderen Zwecke verarbeiten und nutzen könnte.[32] Der Verarbeitungsspielraum ist letztendlich identisch mit dem des Unternehmers, der die Daten übermittelt hat.[33] Bewertungsmaßstab für die weitere Verarbeitung durch den Unternehmer, der die Daten erhalten hat, ist allein dessen Einschätzung, ob schutzwürdige Interessen der Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegen könnten. Es wäre ihm unter anderem nicht verwehrt, die empfangenen Daten einer weiteren Stelle zu übermitteln. Die Intransparenz für die Betroffenen ist offensichtlich und nicht hinnehmbar. Unterstellt man dem Gesetzgeber an dieser Stelle kein achtloses Vorgehen hinsichtlich der Wahrung des Persönlichkeitsschutzes, drängt sich zumindest der Verdacht auf, dass er solche verwirrenden und überflüssigen Regelungen bewusst in Kauf genommen hat. So hätte der Sachverhalt der Funktionsübertragung, der bereits seit geraumer Zeit Anlass zu Diskussionen bietet, bei der letzten Reform zum BDSG geregelt werden können. Zur Wahrung des Persönlichkeitsschutzes der Betroffenen könnten die Unternehmer im Rahmen der Funktionsübertragung eine Zweckänderung zwar vertraglich ausschließen – ob sie dies tun, ist aber eine andere Frage, da eine gesetzliche Verpflichtung hierzu nicht vorhanden ist. Für die Funktionsübertragung gibt es durchgängig –angefangen beim Schriftformerfordernis und der geforderten Dokumentation der Prüfung- keine gesetzlichen Regelungen, die die Interessen der Betroffenen schützen. Ergänzend sei angemerkt, dass die Auftragsdatenverarbeitung auch einer Zulässigkeitsprüfung anhand des § 28 Abs. 1 S. 1 Nr. 2 BDSG standhalten würde. Der Sache nach entscheidet vor allem die Neufassung des § 11 BDSG, dass die schutzwürdigen Interessen der Betroffenen berücksichtigt werden. Diese Konstruktion ist einer internen Datenverarbeitung durch (ebenfalls weisungsgebundene) Mitarbeiter vergleichbar, die keine Zweckänderung erlaubt.

3. Vertragsfreiheit

Eine vermittelnde Meinung beruft sich wegen der letztgenannten Gründe auf die sogenannte Vertragstheorie. Danach soll § 11 BDSG insoweit extensiv ausgelegt werden, dass jede denkbare Fallgestaltung mittels eines Auftragsdatenverarbeitungsvertrages geregelt werden kann, da in diesem Falle sichergestellt sei, dass sämtliche gesetzlich geforderten Voraussetzungen eingehalten werden.[34] So könnte beispielsweise die Personaldatenverwaltung vollständig an ein anderes Unternehmen ausgelagert werden, wenn sämtliche Voraussetzungen des § 11 BDSG erfüllt werden und die Verantwortung der auslagerten Stelle bestehen bliebe. Diese Auffassung scheint auf den ersten Blick eine angemessene Alternative darzustellen, sofern dem Auftraggeber umfassende Weisungsbefugnisse verbleiben und er in sämtliche Entscheidungsbefugnisse eingebunden ist. In diesem Fall könnte tatsächlich überlegt werden, auf das für die Auftragsdatenverarbeitung geforderte einschränkende Kriterium der bloßen „Hilfsfunktion“ zu verzichten.[35] Es muss allerdings berücksichtigt werden, dass nicht nur der geschriebene Vertrag die Rechte der Betroffenen wahrt, sondern vor allem die praktische Durchführung des Vertrages. Eine Auftragsdatenverarbeitung soll insgesamt nur in Betracht kommen, wenn der Auftraggeber auch tatsächlich in der Lage ist, dem Auftraggeber jeden Arbeitsschritt vorzuschreiben.[36] Gerade diese Anforderung erscheint jedoch etwa bei Auslagerung der Personaldatenverwaltung , Bonitätsbewertungen oder Buchhaltung aus praktischen Gründen fraglich.[37] Dies zeigen etwa die eingangs dargestellte Diskussion um die rechtliche Einordnung der Personaldatenverwaltung und die umstrittene Frage, inwieweit es sich bei den Bereichen des Werkschutzes oder der Detektivarbeit um Auftragsdatenverarbeitung handelt: Liegt es insbesondere bei Detektivarbeit nicht außerhalb der Lebenserfahrung, dass sämtliche Überwachungsschritte exakt vorgegeben werden?[38] Weiterhin muss kritisch hinterfragt werden, ob durch diese Ausgestaltung eines Auftragsdatenverarbeitungsvertrag „Verwertungsgrenzen“ umgangen werden.[39] Die Grenze ist in diesem Falle erreicht, wenn eine Auftragsdatenverarbeitung keine tatsächliche Weisungsbefugnis enthält, sondern nur auf dem Papier besteht. Problematisch ist in dem gesamten Kontext, dass Wirtschaftsvertreter im Arbeitsbericht „konzerninterner Datenverkehr“ die Auffassung vertreten,[40] dass einerseits das Kriterium der Entscheidungsbefugnis im Rahmen der Auftragsdatenverarbeitung nicht zu eng bewertet werden dürfte und andererseits eine vertragliche Verantwortungsübernahme für nicht gerechtfertigt halten. Der Begründung lässt sich entnehmen, dass die Wirtschaftsvertreter insgesamt für einen größeren Gestaltungsspielraum bei der Auftragsdatenverarbeitung plädieren mit dem Verweis darauf, dass bei einer Funktionsübertragung sogar eine Zweckänderung der Datennutzung erlaubt sei– daher seien die Rechte der Betroffenen bei Annahme einer Auftragsdatenverarbeitung umfassender geschützt.[41] Diese Ausführungen implizieren, dass die Wirtschaftsvertreter den

Aufsichtsbehörden nahe legen, einen eigenen Ermessenspielraum bei Auftragsdatenverarbeitung zu akzeptieren, da sie ansonsten bei den zu regelnden Sachverhalten weiterhin von Funktionsübertragung mit (grundsätzlich) erlaubter Zweckänderung der Datennutzung ausgehen.[42]

IV.Fazit

Die obigen Ausführungen zeigen, dass bei den rechtlichen Möglichkeiten der Funktionsübertragung vieles ungeklärt ist und eine enorme Gefährdung für den Persönlichkeitsschutz der Betroffenen beinhalten. Informationelle Selbstbestimmung muss jedoch bedeuten, dass die Betroffenen sicher sein können, dass derjenige, dem sie ihre Daten anvertraut haben, die verantwortliche Stelle bleibt und ihre Daten ebensowenig einer undurchsichtigen Zweckänderung durch Dritte unterliegen. Nur auf diese Weise können die Betroffenen über die Preisgabe und Verwendung ihrer Daten selbst bestimmen. Anderenfalls wäre die Verfügungsbefugnis über die eigenen Daten in das Ermessen eines Dritten gelegt, der aufgrund seiner wirtschaftlichen Belange nicht in der Lage ist, über die schutzwürdigen Interessen der Betroffenen objektiv zu entscheiden. Hierfür fehlen konkrete Vorgaben bezüglich der Datenweitergabe an Dritte, insbesondere der gesetzliche Ausschluss der Zweckänderung bei einer Funktionsübertragung. Zu berücksichtigen ist insgesamt, dass sich der Gesetzgeber aufgrund der Konkretisierung sowie der Bußgeldandrohung letztendlich ebenso zur Verschärfung des § 11 BDSG entschlossen hat. Das gesetzgeberische Ziel, durch Kontroll- und Dokumentationspflichten, den datenschutzgerechten Umgang mit personenbezogenen Daten sicherzustellen, wird nun völlig konterkariert, wenn sich die Zulässigkeit der Datenübermittlung und Zweckänderung allein anhand einer „summarischen Prüfung“ durch die Unternehmer dahingehend bemisst, ob schutzwürdige Interessen des Betroffenen verletzt sein könnten.[43] Denn vornehmlich muss sich die Frage stellen, unter welchen Voraussetzungen die schutzwürdigen Interessen des Betroffenen nicht verletzt sind. Dies kann im Sinne der Gesetzesintention nur dergestalt ausgelegt werden, dass die Mindestanforderungen des § 11 BDSG eingehalten werden: Die Weitergabe von Daten darf nur in schriftlicher Form erfolgen, der Unternehmer muss sich von der sorgfältigen Arbeitsweise des anderen Datenverarbeiters überzeugen, er darf nicht aus der Haftung entlassen werden und die einzelnen Maßnahmen, insbesondere technischer und organisatorischer Natur müssen nachprüfbar fixiert werden. In der Praxis enthalten Auftragsdatenverarbeitungsverträge häufig eine zusätzliche Vertragsstraferegelung eingebaut, um die Wichtigkeit der Betroffenenrechte nochmals zu untermauern. Bei der Funktionsübertragung sind solche Kriterien per Gesetz nicht gefordert. Unter Berücksichtigung dessen, dass mit der Weitergabe von Daten an Dritte (= Übermittlung gemäß § 3 Abs. 4 Nr. 3 BDSG) das Persönlichkeitsrecht stärker betroffen ist als wenn die Daten einem weisungsgebundenen Auftragnehmer überlassen werden, ist die Funktionsübertragung äußerst bedenklich: Während die „Hilfsfunktion“ der Datenverarbeitung nur unter engen gesetzlichen Voraussetzungen zugelassen wird, werden darüber hinaus gehende Tätigkeiten lediglich an dem vagen Merkmal der schutzwürdigen Interessen gemessen. Wie oben bereits ausgeführt, hat der Gesetzgeber die Funktionsübertragung im Rahmen der letzten BDSG-Reform nicht geregelt und die weite Auslegung der Übermittlungstatbestände in Kauf genommen. So wäre es beispielsweise möglich gewesen - wie im Modernisierungsgutachten vorgeschlagen - zumindest eine Information der Betroffenen mit Widerspruchsmöglichkeit aufzunehmen.[44] Demgegenüber hat der Gesetzgeber die Anforderungen an die Auftragsdatenverarbeitung verschärft. Dieser Widerspruch ist bizarr: Eine durch vollständige Aufgabe der Weisungs- und Kontrollmöglichkeiten sowie Zweckänderungsgefahr bedingte eingriffsintensivere Datenverarbeitung wird durch eine unbestimmte Regelung wie § 28 Abs. 1 S. 1 Nr. 2 BDSG legitimiert während die bereits vor der Reform reglementierte und das Persönlichkeitsrecht bewahrende Auftragsdatenverarbeitung weiter eingeschränkt wird. Über das Ansinnen des Gesetzgebers können nur Mutmaßungen angestellt werden.

Die vermittelnde Meinung („Vertragstheorie“) hat zwar den Vorteil, dass die Schwächen der Funktionsübertragung insoweit ausgeglichen werden, dass der Auftraggeber für die Datenverarbeitung des Auftragnehmers verantwortlich bleibt und sämtliche Regelungen des § 11 BDSG –bei Übertragung einer gesamten Aufgabe– eingehalten und kontrolliert werden müssen. Auf der anderen Seite muss allerdings bedacht werden, dass sich der bei Vertragsabschluss und während der Vertragsdurchführung angelegte Maßstab ausschließlich auf die tatsächliche Ausführung des Vertrages beziehen kann. Ein Unternehmer müsste sich kritisch fragen, ob er dem Dienstleister sämtliche Arbeitsschritte derart detailliert vorgeben kann, dass seine Entscheidungsbefugnis unangetastet und unmissverständlich ist. Diese Vorgehensweise wird freilich von dem Manko begleitet, dass abermals allein die Einschätzung des Unternehmers entscheidend sein soll – ohne objektiven Bewertungsmaßstab oder Einflussmöglichkeit der Betroffenen. Besonders kritisch zu betrachten sind ferner die Tendenzen, die auf das Merkmal der Weisungsbefugnis in einem Auftragsdatenverarbeitungsvertrag verzichten wollen.[45] Damit würde ein wichtiges gesetzliches Kriterium des § 11 BDSG entfallen, welches gerade sicherstellt, dass dessen Anforderungen eingehalten und die Daten im Sinne des Auftraggebers verarbeitet werden. Die Auftragsdatenverarbeitung wäre außerdem ausnahmslos ad absurdum geführt, wenn das Kriterium der fehlenden Entscheidungsmacht zu erleichterten Bedingungen beim Outsourcing führen soll. Der Unternehmer müsste seinem Partner also lediglich mehr Spielraum bei der Verarbeitung einräumen, um seine Dokumentations- und Kontrollpflichten zu umgehen? Falls nun das Argument angeführt werden sollte, es sei ja klar, dass in diesem Falle das schutzwürdige Interessen des Betroffenen überwiegt, kann man entgegenhalten, dass dann auch nichts dagegen einzuwenden ist, dies transparent und ausdrücklich gesetzlich zu fixieren. Die momentane verwirrende Gesetzeslage lässt eine viel zu große Spanne für Interpretationen. Eine Interessenabwägung, die sich an dem im erhöhten Maße schutzwürdigen

Belangen der Betroffenen misst,[46] wird letztendlich nur durch klare gesetzliche Regelungen zu bewerkstelligen sein und nicht durch Einschätzungen seitens der Unternehmer. Dies zeigt sich bereits daran, dass der Gesetzgeber sogar bezüglich der Auftragsdatenverarbeitung darauf hingewiesen hat, dass in der Praxis ohne entsprechende gesetzliche Verpflichtung regelmäßig keine Kontrolle stattfindet.[47]

1 Siehe Gabel in: Taeger/Gabel, § 11 BDSG Rn. 16 bezüglich einer gesetzlich vorgegebenen Möglichkeit, in unkomplizierter Weise an den Vorteilen einer arbeitsteiligen Wirtschaft teilzuhaben.

2 Gola/Schomerus, 10. Auflage, § 11 BDSG Rn. 3.

3 Zur „Hilfsfunktion“ siehe Gabel in: Taeger/Gabel, § 11 BDSG Rn. 14; Petri in: Simitis , 7. Auflage, § 11 BDSG Rn. 22.

4 Zur “rechtlichen Einheit” siehe Gola/Schomerus, 10. Auflage §11 BDSG Rn. 4.

5 Siehe zu den Betroffenenrechten Petri in: Simitis, 7. Auflage, § 11 BDSG Rn. 23.

6 Gola/Schomerus, 10. Auflage, § 11 BDSG Rn. 9.

7 Gabel in: Taeger/Gabel; § 11 BDSG Rn. 23 mit Verweis auf die Möglichkeit einer weiten Auslegung der Auftragsdatenverarbeitung.

8 Petri in: Simitis, 7. Auflage, § 11 BDSG Rn. 37 mit Verweis auf die Praxis, in der es eher unwahrscheinlich sei, dass innerhalb von Konzernstrukturen der Auftraggeber die volle Verantwortung für Personalentscheidungen und Personaldatenverarbeitung behalte; siehe zum Ganzen auch Gola/Schomerus, 10. Auflage § 11 BDSG Rn. 9 und Gola, Handbuch zum Arbeitnehmerdatenschutz, Rn. 992.

9 Dieser Arbeitsbericht behandelt ausschließlich den konzern**internen** Datentransfer und protokolliert die Auffassungen des Regierungspräsidium Darmstadt und Wirtschaftsvertretern zum Thema „Funktionsübertragung im Konzern“; abrufbar unter https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Datenschutzrecht/Inhalt/Personalwesen/Inhalt/5_Beschaeftigtendatenschutz_Konzern/arbeitspapier_ad_hoc_idv.pdf

10 Arbeitsbericht „konzerninterner Datenverkehr“, S. 3.

11 Arbeitsbericht „konzerninterner Datenverkehr“, S. 3/4.

12 Arbeitsbericht „konzerninterner Datenverkehr“, S. 4.

13 BT-Drs. 16/12011, S. 40.

14 BT-Drs. 16/12011, S. 40.

15 BT-Drs. 16/12011, S. 40.

16 BT-Drs. 16/12011, S. 40.

17 Arbeitsbericht „konzerninterner Datenverkehr“, S. 7 ff.; Gabel in: Taeger/Gabel, § 11 BDSG Rn. 14, der darauf verweist, dass die allgemeinen Regelungen zur Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten gelten; Weichert, DuD 2010, S. 683.

18 Wedde in: Däubler/Klebe/Wedde/Weichert, 3. Auflage, § 28 BDSG Rn. 14.

19 Siehe hierzu die nachfolgenden Ausführungen unter III.2a.

20 Simitis in: Simitis, 7. Auflage, § 28 BDSG Rn. 53, 54.

21 Simitis in: Simitis, 7. Auflage, § 28 BDSG Rn. 55.

22 Siehe hierzu auch Simitis in: Simitis, 7. Auflage, § 28 BDSG Rn. 82, der auf die Unzulässigkeit einer „freien Zirkulation“ Bezug nimmt.

23 Simitis in: Simitis, 7. Auflage, § 28 BDSG Rn. 101.

24 Siehe zur Zweckänderung: Arbeitsbericht „konzerninterner Datenverkehr“, S. 9 und in diesem Beitrag die nachfolgenden Ausführungen unter III.2b.

25 Siehe hierzu Arbeitsbericht „konzerninterner Datenverkehr“, S. 6 mit Verweis auf die Zweckbestimmung und Erforderlichkeit, wenn der Arbeitsvertrag ein Tätigwerden des Arbeitnehmers auch in anderen Konzernunternehmen vorsieht.

26 Siehe hierzu auch Weichert, DuD 2010, S. 683.

27 Simitis in: Simitis, 7. Auflage, § 28 BDSG Rn. 108.

28 Als Denkanstoß kann in diesem Falle ebenso angeführt werden, dass die Frage „Muss dies sein?“ nicht ungewöhnlich ist und beispielsweise ebenso unter Datensicherheitsaspekten hinsichtlich der Verarbeitung personenbezogener Daten auf Notebooks (und zwar innerhalb der verantwortlichen Stelle!) von dem Landesdatenschutzbeauftragten von Bremen gestellt wird: Siehe hierzu die Ausführungen in Gola/Schomerus, 10. Auflage, § 9 BDSG Rn. 17 mit Verweis auf den 15. TB des Landesdatenschutzbeauftragten Bremen: „Eine Verarbeitung von personenbezogenen Daten auf tragbaren PCs darf nur erfolgen, wo dies aufgrund der Aufgaben unvermeidbar ist“.

29 Siehe zur Unbestimmtheit unter anderem Taeger in: Taeger/Gabel, § 28 BDSG Rn. 62.

30 Simitis in: Simitis, 7. Auflage, § 28 BDSG Rn. 129.

31 Siehe zum konzerninternen Datenaustausch und der Auffassung der Aufsichtsbehörden: Arbeitsbericht „konzerninterner Datenverkehr“, S. 8.

32 Gemäß § 28 Abs. 2 Nr. 1 BDSG ist eine Übermittlung und Nutzung und gemäß § 28 Abs. 5 BDSG eine Verarbeitung und Nutzung für andere Zwecke zulässig, soweit es zur Wahrung berechtigter Interessen erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt.

33 Siehe auch Wedde in: Däubler/Klebe/Wedde/Weichert, 3. Auflage, § 28 BDSG Rn. 162.

34 Gabel in: Taeger/Gabel, § 11 BDSG Rn. 15. Siehe auch Weichert, DuD 2010, S. 683, der darauf verweist, dass schutzwürdige Interessen durch Maßnahmen gewährleistet werden können, die in § 11 BDSG vorgesehen sind.

35 Siehe zum Merkmal der “Hilfsfunktion” eines Dienstleisters, der Daten im Auftrag gemäß § 11 BDSG verarbeitet: Gabel in: Taeger/Gabel, § 11 BDSG Rn. 14 sowie Petri in: Simitis, 7. Auflage, § 11 BDSG Rn. 22.

36 Petri in: Simitis, 7. Auflage, § 11 BDSG Rn. 20 mwN.

37 Siehe zu diesen „Outsourcing-Sachverhalten“ Petri in: Simitis, 7. Auflage, § 11 BDSG Rn. 25 ff.

38 Siehe hierzu Gabel in: Taeger/Gabel, § 11 BDSG Rn. 20, der bei Detektivarbeit von Funktionsübertragung ausgeht, wenn der Detektiv selbst bestimmt, wie er den Auftrag ausführt und welche Mittel er einsetzt - mit Verweis auf den Bericht des Innenministeriums von Baden-Württemberg über die Tätigkeit der Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich. Gola hingegen (Handbuch zum Arbeitnehmerdatenschutz, 5. Auflage, Rn. 993) verweist darauf, dass sowohl Auftragsdatenverarbeitung und Funktionsübertragung in Betracht komme; Petri in: Simitis, 7. Auflage, § 11 BDSG Rn. 41 geht wiederum davon aus, dass regelmäßig eine Funktionsübertragung in Betracht kommt.

39 Simitis in: Simitis, 7. Auflage, § 28 BDSG Rn. 140 verweist auf die Unzulässigkeit, Verwertungsgrenzen

und Übermittlungsschranken unter Zuhilfenahme einer Auftragsdatenverarbeitung zu umgehen.

40 S. 4 und 9 des Arbeitsberichts „konzerninterner Datenverkehr“.

41 Arbeitsbericht „konzerninterner Datenverkehr“, aaO.

42 Arbeitsbericht „konzerninterner Datenverkehr“, S. 9: „Bei einer Funktionsübertragung sei nämlich zu berücksichtigen, dass der Funktionsübernehmer als verantwortliche Stelle einen umfassenderen Spielraum bei der Nutzung der Daten erhalte (z.B. sie im Rahmen von § 28 Abs. 2, 3 BDSG für andere Zwecke nutzen könne), so dass die Rechte der Betroffenen bei Annahme einer Auftragsdatenverarbeitung ggf. umfassender geschützt seien als bei Annahme einer Funktionsübertragung (bzw. es bedürfe nicht besonderer vertraglicher Regelungen, um die Zweckänderung auszuschließen).“

43 Zur summarischen Prüfung siehe Simitis in: Simitis, 7. Auflage, § 28 BDSG Rn. 129.

44 Gutachten im Auftrag des Bundesministeriums des Innern zur Modernisierung des Datenschutzrechts (Roßnagel, Pfitzmann, Garstka), S. 125.

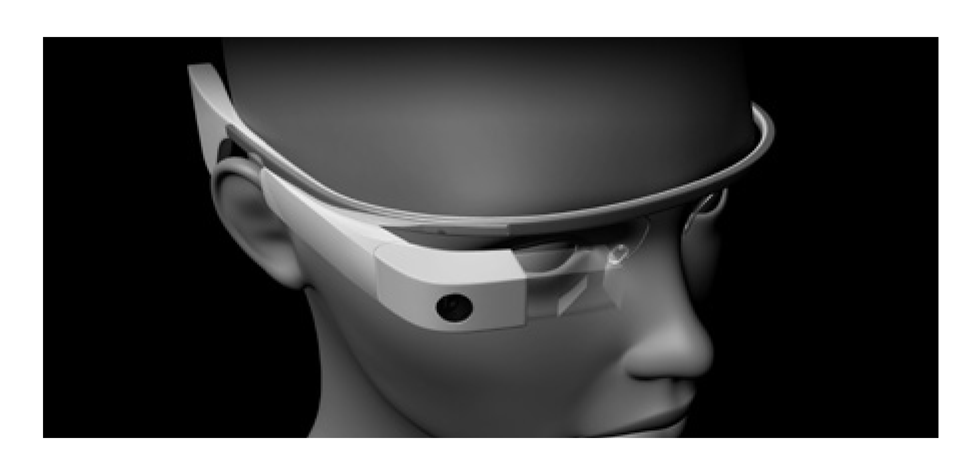
45 Siehe oben unter III.3.

46 Siehe hierzu Wedde in: Däubler/Klebe/Wedde/Weichert, 3. Auflage, § 28 BDSG Rn. 162.

47 Siehe oben unter III.1 und BT-Drs. 16/12011, S. 40.

Thilo Weichert

Google Glass, IT-Brillen und informationelle Selbstbestimmung



April 2013 stellte Robert Scoble, US-amerikanischer Technik-Blogger, früherer Microsoft-Angestellter und nun Werbeträger für Google, im Kongress-Zentrum am Alexanderplatz in Berlin auf der Technologiemesse Next „Google Glass“ in Deutschland vor: „Sie hat mein Leben verändert. Ich werde keinen Tag mehr verbringen, ohne sie zu tragen“.

Bei Google Glass handelt es sich um eine Art Brille ohne Gläser, an der am schmalen Bügel ein Quader, eine Art Prisma, angebracht ist. Google Glass bietet viele Funktionen, die komplexe Smartphones bieten. Statt eines Displays gibt es einen direkt am Auge angebrachten Minibildschirm. Scobles Brille war die 107. von zweitausend 1.500 Dollar kostenden Prototypen, die insbesondere für Werbe- und Erprobungszwecke ausgeliefert wurden. Der Miniprojektor vermittelt das Gefühl, im rechten oberen Blickfeld einen ca. 20 Zentimeter großen Bildschirm zu sehen. Zur Bildqualität gibt Google an, sie sei genauso gut, als würde man in 2,4 Meter Entfernung (8 Fuß) vor einem 63 Zentimeter (8 Zoll) großen HD-Schirm stehen. Die Brille reagiert auf Sprache und Kopfbewegungen. Künftig soll das Produkt auch mit Augenbewegungen gesteuert werden können. Geht eine E-Mail ein, so wird diese am Bildschirm angezeigt. Mit einer integrierten 5-Megapixel-Kamera lassen sich Fotos und Videos erstellen. Bei Videos gibt es eine Auflösung von 720p, was der kleinsten HD-Auflösung entspricht. Der Flash-Speicher soll 16 Gigabyte groß sein; 12 Gigabyte davon stehen den Nutzenden zur Verfügung. Über ein Mikrophon sind Spracheingaben und Tonaufnahmen möglich; das Starten erfolgt durch die Eingabe „Okay, Glass“. Tonausgaben erfolgen nicht über Lautsprecher, sondern vom Bügel direkt auf den Schädelknochen – ein Verfahren, was bisher bei Hörgeräten verwendet wird. Glass hat umfassenden Zugang zum Internet, zwecks Hoch- und Runterladen von Texten, Dokumenten, Bildern und akustischen Samples, zwecks Eingabe und Abruf. Sämtliche Daten – Inhalte, Verkehrsdaten und Personenzuordnungen – laufen über Server von Google und werden von dem US-Unternehmen gespeichert und ausgewertet. Ein Lokalisierungsdienst ermöglicht es, den eigenen Standort auf einer Karte anzuzeigen oder den Weg zu einem festgelegten Ziel zu weisen. Per Gesichtserkennung könnte die Brille dem Halter mitteilen, wer ihm – wahrscheinlich – gerade gegenübersteht. Der Akku soll ohne Nachladen einen ganzen Tag durchhalten. Videoverbindungen wie sog. Hangouts und Videoaufnahmen verbrauchen mehr Strom und leeren den Akku schneller. Geladen wird über ein mitgeliefertes Ladegerät mit Mikro-USB-Anschluss. In den Hinweisen wird erläutert, dass Kinder unter 13

Jahren die Brille nicht nutzen sollten, da sie ihre Sehentwicklung beeinträchtigen könne. Auch wer seine Augen mit einem Laser operieren ließ, solle Glass nicht unbedingt nutzen.

Natürlich wurde Google Glass weltweit nicht zuerst in Deutschland vorgestellt, sondern einen Monat zuvor in den USA auf der TED-Konferenz durch den Google-Gründer Sergey Brin. Die Brille befreit von der Notwendigkeit, ein Smartphone in die Hand zu nehmen. Das Produkt zielt auf eine Verschmelzung der analogen mit der digitalen Welt. Gebückt befasste sich Brin bei der Präsentation erst mit einem klassischen Smartphone: „Haben wir dazu unseren Körper? Um herumzustehen und ein eigenschaftsloses Stück Glas zu reiben? Für mich fühlt sich das an wie eine Entmannung.“ Hände, Augen und Ohren des Menschen sollten befreit werden. Aufrecht nutzte er dann sein Glass. Ein offizielles Werbevideo zeigt dem Träger die aktuellen Termine an, dann eine Wettervorhersage, dann eine Kurznachricht eines Freundes in einem Buchladen, die mündlich beantwortet, in Text übersetzt und der Text versendet wird. Glass bestellt dann, vor dem Plakat eines Popkonzerts stehend, hierfür Eintrittskarten. Am Ende steht der Held abends auf dem Dach eines Hauses, erhält einen Videoanruf seiner Freundin, die auf ihrem Computerbildschirm den Sonnenuntergang durch seine Augen betrachtet, während er Ukulele spielt und sie durch ein kleines Fenster im Blickfeld beobachtet. Beruhigend teilte Google bei der Vorstellung der Öffentlichkeit mit, Anwender von Glass vorerst nicht mit Werbung behelligen zu wollen. Doch Glass soll natürlich zur Produktvermarktung eingesetzt werden. Es soll der einkaufenden Frau – so das Werbevideo eines US-Lebensmittelkonzerns, ein Mann würde durch solch einen Clip wohl „entmannt“ – nicht nur mitteilen, welche Waren im Kühlschrank fehlen, sondern auch, in welchem Laden die fehlenden Produkte in welchem Regal zu finden sind und wie die Frau am schnellsten dorthin findet.

Wenige Tage nach Präsentation der Brille wurde verbreitet, dass Glass bereits gehackt worden sei. Der unter dem Spitznamen Saurik bekannte Softwareentwickler Jay Freeman erklärte, er habe es innerhalb von zwei Stunden geschafft, sich vollen Zugriff auf das Betriebssystem zu verschaffen. Dass das Gerät „hackbar“ ist, wurde von Google auch nicht bestritten. Google-Manager propagieren selbst das Spielen mit der Technik, um Soft- und Hardware weiter zu entwickeln. Unklar ist, was der Jailbreak für die Google-Brille ermöglicht, etwa ob sich das von Google verfügte Verbot des Verkaufs oder Verleihs der Testgeräte umgehen lässt. Google behält sich in den Nutzungsbedingungen zur „Explorer Edition“ der Datenbrille vor, das Gerät aus der Ferne zu „deaktivieren“, sollte es verkauft oder weitergereicht werden. Möglich wäre das dadurch, dass diese, ähnlich wie ein Android-Handy, über einen Google-Account aktiviert werden muss. Würde eines der Testgeräte mit einem neuen Account verknüpft, würde dies vermutlich von Google registriert.

Ende 2013 soll Glass auf den US-amerikanischen Markt kommen, dann aber bald auch in Europa. Prophylaktisch wurde Glass schon – vielleicht ein kluger Werbegag – für Stripclubs, Casinos, Multiplexkinos und für den Straßenverkehr in West Virginia verboten. Von der Pornoindustrie kamen dagegen positive Signale, erleichtert doch Glass das Erstellen von Filmen aus einer sehr subjektiven Perspektive. Der Initiator von „Stop the Cyborgs“ wiederum, der sich im Netz Adam nennt, erklärte Glass zum Einstieg in die Überwachungsgesellschaft und fordert überwachungsfreie Zonen, „in denen Menschen frei und unbekümmert reden können“.

Glass ist ein ziviles Produkt, das seine Vorläufer im Militär- und Sicherheitsbereich hat. Beim US-Militär sind Helmkameras für kämpfende Einheiten weit verbreitet. Die Firma Taser rüstet nun Polizisten in den USA mit winzigen Videokameras aus, die an einer Art Brillengestell befestigt werden und mit denen diese ihre Einsätze dokumentieren. Bei der Auswertung eines mehrmonatigen Feldversuchs im kalifornischen Rialto mit dem „Axon Flex“ genannten System ergab sich, dass die Zahl der Beschwerden gegen Polizisten abnahm wie auch die Zahl der Fälle, in denen die Beamten Gewalt anwendeten. Die Datenbank, auf der die Bilder von den Polizeieinsätzen aufgespielt werden, unterliegt bisher nicht der staatlichen Kontrolle, sondern dem Privatunternehmen Taser. Taser vertraut auf Amazon, das die Server für Evidence.com zur Verfügung stellt. Richtlinien, geschweige denn eine gesetzliche Grundlage für den Einsatz der Technik, gibt es nicht. Videodokumentation sichert nicht zweifelsfrei echte Bilder. 2010 wurde die Polizei in London überführt, Bilder einer Überwachungskamera für ein Gerichtsverfahren manipuliert zu haben. Dies ist auch mit der Brillentechnik möglich. Nach Angaben von Taser haben die Polizeibehörden von Pittsburgh, Salt Lake City, der Bahn Bay Area Rapid Transit und andere das System bestellt. Auch in Deutschland kommen Helmkameras bei Einsätzen von Spezialkommandos zum Einsatz. Zum Zweck der Eigensicherung bei Personen- und Fahrzeugkontrollen werden Kameras eingesetzt, die nicht am Körper des Polizisten, sondern am Einsatzfahrzeug installiert sind.

Google Glass ist eine logische Weiterentwicklung vorhandener Technik. Während jedoch beim Filmen und Fotografieren mit Smartphone und Minikamera noch eine bewusste und erkennbare Aktivität des Erfassers nötig ist, fällt dies bei Glass fort. Für die Erfassten ist beim Brilleneinsatz nicht mehr ansatzweise erkennbar, wann gefilmt wird, ja dass überhaupt gefilmt werden könnte.

Aus Datenschutzsicht ist die neue Technologie eine Herausforderung: Es erfolgt nicht nur eine Erfassung der Daten der Anwendenden, sondern auch von dritten Personen, die mit dem Brillenträger überhaupt nichts zu tun haben müssen und die regelmäßig keine Kenntnis von der Aufzeichnung, vor allem von Ton und Bild, haben. Die Betroffenen können erst recht keine Vorstellung haben, welche sie betreffenden weiteren Datenverarbeitungen stattfinden, etwa ob Gesichtsbilder oder Sprachaufzeichnungen gespeichert werden oder per Mustererkennung mit Musterdatenbanken abgeglichen werden, was eine individuelle Zuordnung ermöglicht, oder ob vom Anwender derartige Zuordnungen vorgenommen werden. Zu Ton und Bild werden Ort und Zeit zugespeichert, möglicherweise auch ganze Profile - etwa aus sozialen Netzwerken.

Die rechtliche Verantwortlichkeit für die Nutzung von Glass liegt zunächst

bei der Person, die die Brille trägt und bedient. Erst hinsichtlich der weiteren Speicherung und Verarbeitung entsteht eine ergänzende Verantwortlichkeit von Google. Möglichkeiten, Google den Verkauf oder den Vertrieb von Glass in Deutschland zu verbieten, bestehen derzeit rechtlich nicht. Auch der Besitz oder das Tragen von Glass – offline – ist rechtlich nicht angreifbar. Beim Einsatz von Glass kann es jedoch zu massiven Rechtsbeeinträchtigungen kommen.

Bisher besteht eine explizite Regelung zum Einsatz von Glass durch Privatpersonen nicht. Doch muss generell von einer Anwendbarkeit des Bundesdatenschutzgesetzes (BDSG) ausgegangen werden, da – anders als etwa bei durchlaufenden Bildern einer PKW-Außenkamera – mit Glass eine gezielte Datenerhebung und -speicherung von dritten Personen erfolgt, bei der eine Beschränkung auf persönlich-familiäre Zwecke nicht erfolgt. Am ehesten anwendbar ist § 6b BDSG zur Videoüberwachung im öffentlichen Raum. Doch ähnlich wie beim Einsatz von Drohnenkameras greift das Regelungskonzept dieser Norm zu kurz: Hinweise an die betroffenen Personen auf die optische Erfassung sind faktisch nicht möglich. Eine Beschränkung der Datenspeicherung im Hinblick auf Zeit, Zweck und Adressaten ist nicht vorgesehen. § 6b BDSG würde zudem allenfalls die optische Erfassung erlauben, in keinem Fall die akustische. Eine solche Aufnahme des „nichtöffentlich gesprochenen Wortes“ und dessen Gebrauch ist nach § 201 Strafgesetzbuch (StGB) strafbar mit „Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe“. Mit den Bildaufnahmen kann eine Verletzung der §§ 23ff. Kunsturhebergesetz (KUG) erfolgen. In jedem Fall stellt die Erfassung von Ton und Bild ohne die Einwilligung der Betroffenen außerdem eine Beeinträchtigung des allgemeinen Persönlichkeitsrechtes und des Grundrechts auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 Grundgesetz (GG) dar.

Ein praktisches Problem besteht für Betroffene darin, dass sie regelmäßig nicht nur nicht feststellen können, dass und wie sie erfasst wurden. Es gibt für sie auch keinen realistischen Weg, um dies in Erfahrung zu bringen. Mangels Möglichkeiten, die Identität des Trägers – also aus juristischer Sicht die der „verantwortlichen Stelle“ – festzustellen, fehlt regelmäßig der faktische Ansatz, um sich rechtlich zur Wehr setzen zu können. Zwar bestehen zivil- und datenschutzrechtlich Auskunftsansprüche der Betroffenen gegenüber dem Glass-Nutzenden. Dieser kann aber relativ folgenlos behaupten, dass keine Erfassung erfolgt sei.

Gibt es für diese Beeinträchtigung keine Legitimation im Einzelfall, so kann – theoretisch – gegen den Einsatz von Glass juristisch vorgegangen werden. Verletzungen des allgemeinen Persönlichkeitsrechts begründen für den Betroffenen gegenüber dem Nutzenden zivilrechtliche Ansprüche nach den §§ 823, 1004 auf Schadenersatz, auf Unterlassung und auf Folgenbeseitigung, also auf Datenlöschung. Datenschutzrechtliche Ansprüche bestehen nach den §§ 34, 35 BDSG auf Auskunft und Löschung. Spätestens nach Widerspruch gegen eine Datenerhebung muss die weitere Erfassung unterlassen werden. Da der Verdacht von Straftaten (§ 201 StGB, § 44 BDSG) bestehen kann, können die Polizei und die Staatsanwaltschaft bemüht werden. Denkbar ist auch, die Polizei im Rahmen der Gefahrenabwehr nach dem Polizeirecht zum Tätigwerden zu veranlassen. Außerdem kann die Datenschutzaufsichtsbehörde nach § 38 BDSG zwecks Ermittlung und Sanktionierung angerufen und tätig werden.

In der Rechtsprechung des Bundesverfassungsgerichtes ist anerkannt, dass schon die begründete Angst, technisch beobachtet zu werden, die Wahrnehmung von Grundrechten beeinträchtigt. Dies gilt für die politischen Freiheitsrechte wie z. B. für das Grundrecht auf Versammlungsfreiheit, aber letztlich für alle anderen Grundrechte. Angesichts dessen ist es nicht ausgeschlossen, dass die Nutzung von Google Glass und vergleichbaren Werkzeugen gesetzlich oder administrativ (z. B. über das Polizeirecht) verboten wird. Derartiges würde aber viele rechtliche Fragen aufwerfen, insbesondere die nach einer hinreichend bestimmten Abgrenzung dessen, was noch erlaubt und was verboten sein soll. Bevor Vertreter staatlicher Stellen, etwa Polizeibeamten, Geheimdienstler oder Steuerfahnder, Glass einsetzen dürfen, bedürfte es in jedem Fall einer ausdrücklichen gesetzlichen Regelung. Dies ist in der Rechtsprechung des Bundesverfassungsgerichtes mit seiner Wesentlichkeitstheorie seit Jahren geklärt.

Wegen der faktischen Schwierigkeit, staatlich-institutionelle Hilfe in Anspruch zu nehmen, stellt sich die Frage, welche Maßnahmen der Selbsthilfe gegen die Erfassung durch Glass zulässig sind. Verhältnismäßig dürfte wohl in jedem Fall die Festhaltebefugnis zwecks Identitätsfeststellung nach § 127 Strafprozessordnung (StPO) sein. Hochinteressant wird voraussichtlich sein, wie gerichtlich im Fall des Selbstschutzes von Betroffenen durch Wegnahme oder gar Zerstörung der Google-Brille entschieden werden wird. Vor Jahren bestätigte die Rechtsprechung immer wieder, dass ein solcher Selbstschutz (zumeist von Polizeibeamten) gegen unzulässiges Fotografieren zulässig war.

Zu hoffen ist, dass all diese rechtlichen Fragen nicht entschieden werden müssen, weil die Menschen in Europa und in Deutschland vernünftig genug sind, den Einsatz dieses persönlichkeitsrechtsverletzenden Gadgets zu unterlassen. Besser als jede institutionelle und rechtliche wäre die gesellschaftliche und kulturelle Sanktionierung. Statt zum Statussymbol zu werden, müsste sich durchsetzen, dass es sich bei Nutzenden von Google Glass um rücksichtslose Idioten handelt. Als erkannte rücksichtslose Idioten wollen nur wenige Menschen durch die Welt laufen. Google könnte es sicher ökonomisch verkraften, wenn Glass ein Flop wird. Aus datenschützerischer und marktpädagogischer Sicht ist genau dies mehr als wünschenswert (Google Glass ist schon gehackt, www. Spiegel. de 28.04.2013; Boie, Zurück aus der Zukunft, Süddeutsche Zeitung (SZ) 26.04.2013, 47; Keine Werbung auf Datenbrille, SZ 24.04.2013, 22; Brauck, Glass-Auge, sei wachsam! Der Spiegel 15/2013, 120; Rosenfelder, Google und wie wir die Welt sehen werden, www. welt.de 16.04.2013; Biermann, Google Glass ist kein Kinderspielzeug, www. zeit.de 16.04.2013; Beuth, Die Polizei dein Freund und Kameramann, www.zeit.de 08.04.2013; Crocoll, Zu viel Durchblick, SZ 02.04.2013, 19; Beuth, Die Anti-Cyborgs, www.zeit.de 21.03.2013).

Karsten Neumann

Meldepflicht von Datenschutzvorfällen – Anforderungen an das Datenschutzmanagement

Nach 4jähriger Praxiserfahrung mit der Meldepflicht von Datenschutzverstößen trügt die allgegenwärtige Empfindung eines Anwachsens von Datenschutzvorfällen. Vielmehr führt die Meldepflicht zunehmend zu einer Aufhellung des Dunkelfeldes – ein Begriff aus der Kriminologie, der all die Fälle zu erfassen versucht, die nicht angezeigt werden und deshalb die Kriminalitätsstatistik als Beschreibung des Hellfeldes ins rechte Licht rücken will. Die Erfahrung und aktuelle Studien belegen, dass vermutlich heute nicht mehr Datenlecks entstehen, sondern nur die bisherigen endlich bekannt werden und somit der Öffentlichkeit ein klareres Bild von der Bedrohungslage geben. Unternehmen sind zunehmend gezwungen, sich mit der Frage auseinanderzusetzen, wie Datenlecks überhaupt bemerkt werden können, um Betroffene wenigstens vor einem drohenden Missbrauch warnen zu können. Datenschutzmanagement wird so zum Pendant einer IT-Sicherheitsstrategie.

Paradigmenwechsel

Mit § 42a BDSG leitete die Novellierung des BDSG 2009[1] einen längst überfälligen Paradigmenwechsel ein. Bei der Beurteilung der Gefährdungen durch einen unberechtigten Abfluss von Informationen steht nicht mehr das Kosten- oder Imageinteresse der verantwortlichen Stelle im Mittelpunkt der Informationspolitik der Unternehmen und der Verschwiegenheitsverpflichtung der Aufsichtsbehörden, sondern das Interesse der Betroffen, um deren Daten es geht. Deren qualifizierte und kostenlose Interessenvertretung wird im Verfahren vor einer Information der Betroffenen durch die zuständige Aufsichtsbehörde wahrgenommen, was zugleich notwendigerweise im Falle eines Datenverlustes unweigerlich die aufsichtsbehördliche Prüfung der Angemessenheit ergriffener Schutzmaßnahmen auf den Plan ruft.

Das amerikanische Konzept der Informationspflichten (Data Breach Notification) wurde durch den deutschen Gesetzeber in Umsetzung einer EU-Richtlinie aufgegriffen und in seinem Anwendungsbereich schrittweise erweitert. So verweist § 93 Abs. 3 Telekommunikationsgesetz auf § 42a BDSG, wenn für den Fall Bestands- und Verkehrsdaten unrechtmäßig zur Kenntnis Dritter gelangen. Entsprechendes gilt nach § 15a Telemediengesetz für Bestands- und Nutzungsdaten nach §§ 14 und 15 TMG und im Sozialrecht gemäß § 83a Sozialgesetzbuch X für Sozialdaten. Vergleichbare Meldepflichten fanden sich aber auch bereits vorher auf landesgesetzlicher Ebene, so zum Beispiel in § 23 DSG MV[2] für öffentliche Stellen, die bisher auf Bundesebene immer noch von der Meldepflicht ausgenommen sind.

Nach Auffassung der Aufsichtsbehörden[3] entsteht die Meldepflicht entgegen dem Wortlaut des Gesetzes nicht erst, wenn die rechtswidrige Übermittlung solcher Daten durch die Stelle festgestellt wurde, sondern bereits wenn anhand von tatsächlichen Anhaltspunkten mit einer gewissen Wahrscheinlichkeit davon ausgegangen werden kann, dass die Daten unberechtigt zur Kenntnis gelangt sein könnten. Auch wenn diese Auffassung von der Gesetzesbegründung nicht gestützt wird, spricht doch die Regelung des § 42a dafür, bereits die Gefährdung oder Möglichkeit rechtswidriger Kenntnis-Erlangung durch Dritte als Anknüpfungspunkt für Ermittlungen, Abwägung und Information zu nutzen.

Die gegenwärtig in der Diskussion stehende EU-Datenschutzgrundverordnung[4] soll auch hier einen Schritt weiter gehen. Gemäß Artikel 31 und 32 des Entwurfes der Kommission soll bereits eine Verletzung von Schutzmaßnahmen innerhalb von 24 Stunden der Aufsichtsbehörde gemeldet und bei einer Wahrscheinlichkeit der Verletzung der Privatsphäre der Betroffenen diese unterrichtet werden müssen.

Die Frage, welches Maß an Verletzung ausreichend sein soll, um eine Meldepflicht auszulösen, hat die Praxis vor enorme Probleme gestellt. Wann führt ein verlorener Generalschlüssel zur Meldepflicht, wenn mit diesem die Personalabteilung betreten werden kann? Muss ein verloren gegangener USB-Stick mit entsprechenden Daten gemeldet werden, wenn dieser 2 Tage später von Unbekannten wieder per Post zugeschickt wurde? Auch die Aufsichtsbehörden stehen vor einer neuen Aufgabe und versuchen gegenwärtig durch die Sammlung von Erfahrungen mit diesen Meldungen Kriterien zu entwickeln, die hoffentlich bald auch durch die Praxis nutzbar werden.

Solange Strafverfolgungsinteressen oder Maßnahmen zur (Wieder-)Herstellung der Datensicherheit es erfordern, kann die Information der Betroffenen abgewartet werden, wenn eine Abwägung mit deren Interesse an einer Verhinderung möglicher Nachteile durch die Datenoffenbarung nicht im Einzelfall überwiegt. Der „Lohn" rechtzeitiger Information ist die Straffreiheit gem. § 42a Satz 6 bezogen auf die Datenschutzverstöße, die gegebenenfalls den Datenabfluss ermöglicht oder begünstigt haben. Diese korrespondiert mit dem strafprozessrechtlichen Grundsatz, dass niemand sich selbst bezichtigen muss, und steht damit unter dem Vorbehalt einer rechtzeitigen Selbstanzeige, also bevor nicht durch die Aufsichtsbehörde bereits Ermittlungen aufgenommen worden sind. Dies hat der Gesetzgeber offensichtlich nicht berücksichtigt, unterstellt er doch in der Gesetzesbegründung die Möglichkeit der Kenntniserlangung durch Hinweise der Aufsichtsbehörden als Ausgangspunkt einer strafbefreienden Selbstanzeige. Wenn die Aufsichtsbehörde allerdings

erst ggf. unter Bezugnahme auf Informationen von Betroffenen die verantwortliche Stelle auf einen Datenverlust aufmerksam machen muss, wird hierdurch zwar die Informationspflicht ausgelöst, die strafbefreiende Wirkung ist damit allerdings verwirkt.

Hieraus entsteht je nach Unternehmensbranche neben dem wirtschaftlichen Interesse des Investitionsschutzes auch ein handfestes rechtliches Interesse, Sicherheitsvorfälle rechtzeitig und möglichst selbst zu erkennen. Diese Aufgabe gestaltet sich jedoch aus der Erfahrung der letzten Jahre von gemeldeten und nicht gemeldeten Sicherheitsvorfällen äußerst schwierig. Sich verlangt von den Unternehmen eine entsprechende Umorganisation ihres Datenschutzmanagementsystems: sowohl organisatorisch, als auch technisch.

Überwachungspflicht

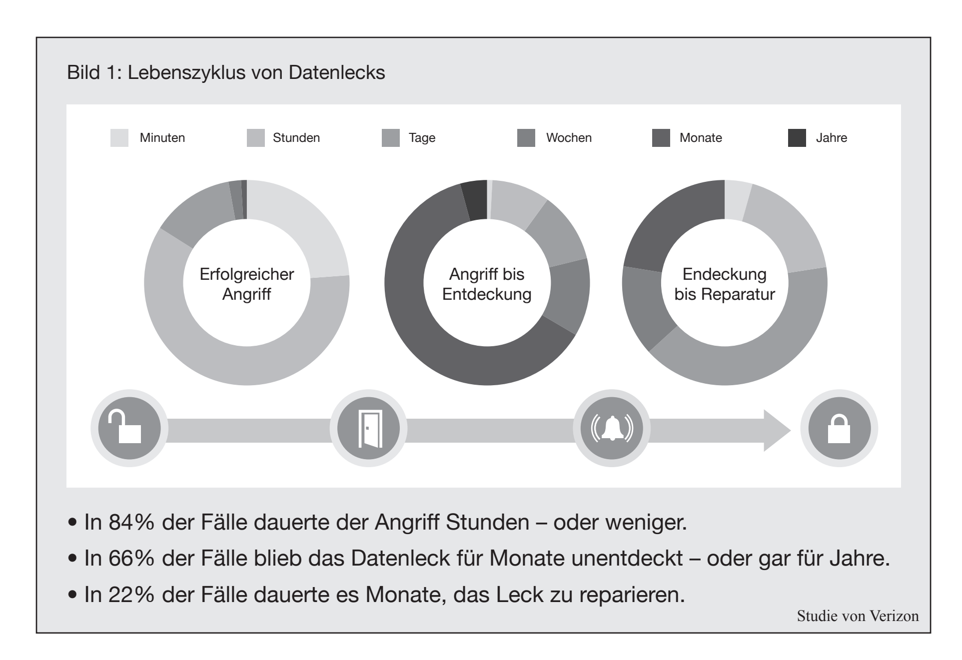
Auch wenn es bisher keine gesetzliche Pflicht zur Durchführung eines Datenschutzmanagementsystems gibt, fand ein Datenschutzkonzept zumindest schon mal Eingang in § 9a BDSG. Wenn man den gesetzgeberischen Auftrag des § 9 BDSG ernst nimmt, geht jedoch kein Weg an einem systematischen Aufbau einer Datenschutzorganisation vorbei. Durch die Einführung eines Datenschutzmanagementsystems wird ein Unternehmen systematisch in die Lage versetzt, alle Prozesse nicht nur rechtlich auf Zulässigkeit zu prüfen, sondern mit dem Verfahrensverzeichnis auch oft erstmalig die technisch-organisatorischen Maßnahmen zu dokumentieren. Hierdurch werden alle Verfahren einer Verarbeitung personenbezogener Daten erfasst, auf die datenschutzrechtliche Zulässigkeit der Datenverarbeitung geprüft, Daten klassifiziert und Sicherheitsmaßnahmen analog dem festgestellten Risiko festgelegt. Hierzu gehören am Ende auch Überwachungssysteme, die eine Datenschutzverletzung identifizieren können. Datenschutzrechtlich zulässige Überwachungsmaßnahmen sind all jene, die zum Aufdecken individuellen Fehlverhaltens geeignet und bestimmt sind. Damit sind sowohl technische Protokollierungen, als auch Zugangssicherungen und Alarmsysteme geeignete Maßnahmen, solange sie verhältnismäßig zum Schutzbedarf der Daten sind. Eine solche Abwägungsentscheidung – die letztendlich auch Gegenstand der Vorab-Kontrolle des betrieblichen Datenschutzbeauftragten ist – setzt mithin eine Schutzbedarfsfeststellung zwingend voraus. Dem Schutzbedarf entsprechend sind die Sicherheitsmaßnahmen auszuwählen. Mit der gesetzgeberischen Beschränkung der Meldepflicht gemäß § 42a auf die dort genannten besonders sensiblen Daten (besondere Arten personenbezogener Daten, personenbezogene Daten, die einem Berufsgeheimnis unterliegen, personenbezogene Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder den Verdacht strafbarer Handlungen oder Ordnungswidrigkeiten beziehen, oder personenbezogene Daten zu Bank- oder Kreditkartenkonten) wurde die Schutzbedarfsklassifizierung für diese Daten als besonders hoch vorweggenommen. Sobald solche Daten in den Verfahren erhoben oder verarbeitet werden, sind Überwachungsmaßnahmen zwingend erforderlich.

Kultur der Verantwortlichkeit

Bei allen Überwachungsmaßnahmen bleibt selbst bei 4-Augen-Verfahren ein Restrisiko menschlichen Fehlverhaltens, dem ein Unternehmen nur noch durch eine Kultur der Verantwortlichkeit entgegentreten kann. Es muss im Unternehmen nicht nur möglich, sondern auch positiv honoriert sein, Fehler einzuräumen und Mängel zu benennen. Eine solche Kultur ist nur durch langjährige Auseinandersetzung und loyale Mitarbeiter auf allen Führungsebenen zu erreichen. Selbst dann müssen interne Systeme für Hinweisgeber es eigenen Mitarbeitern ergänzend ermöglichen, anonym auf Sicherheitsverstöße hinzuweisen. Auch wenn die Anonymität die Aufklärung erschwert und das Risiko von Missbrauch mit sich bringt, sollte das Aufklärungsinteresse im Interesse des Unternehmens und der Betroffenen höher stehen. Solche Möglichkeiten sind durch die Verschwiegenheitspflicht der betrieblichen Datenschutzbeauftragten personell eröffnet, könnten aber schon durch einen Beschwerdebriefkasten beispielsweise im Fahrstuhl technisch einfach umgesetzt werden.

Technische Schutzvorkehrungen

Weit schwieriger und aufwändiger sind die erforderlichen technischen Maßnahmen. Nach einer jüngst veröffentlichten Studie von Verizon, dem „Data Breach Investigations Report 2013“ (DBIR2013)[5], ergab die Untersuchung in 27 Ländern und unterschiedlichsten Geschäftsbereichen ein erschreckendes Bild: die Unternehmen erfahren von einem Datenleck in der Regel zu spät und durch Dritte. So weist der DBIR2012 für den Bereich der Gesundheitswirtschaft[6] aus, dass 84% aller erfolgreichen Angriffen innerhalb von Minuten abgeschlossen sind, in 66% aller Fälle Monate bis Jahre unentdeckt bleiben und es in 22% aller Fälle Monate



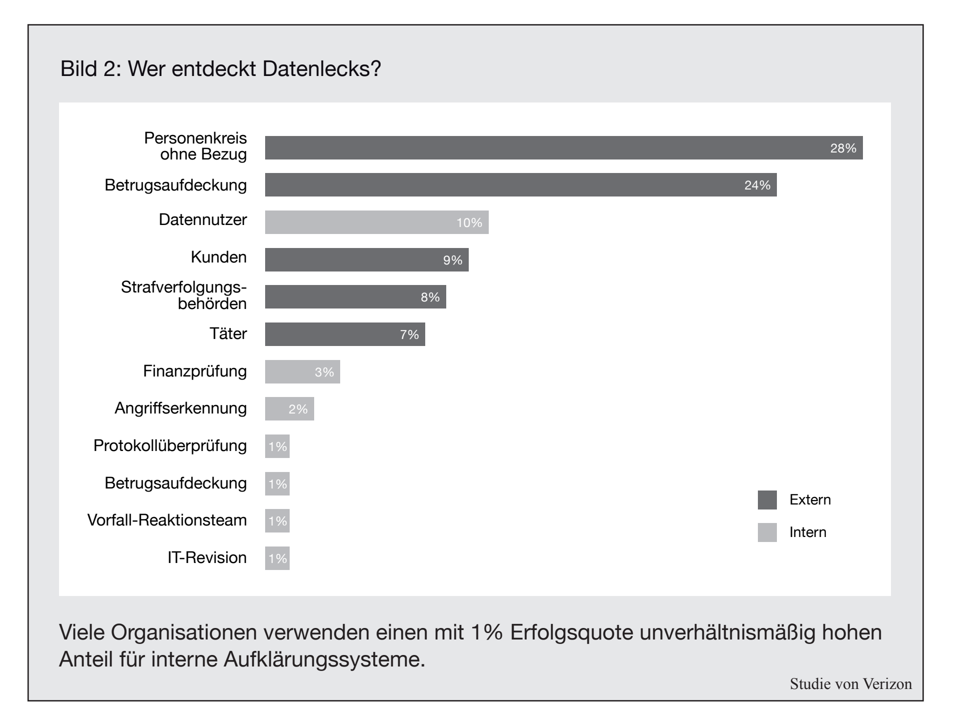


Bild 2: Wer entdeckt Datenlecks?

Viele Organisationen verwenden einen mit 1% Erfolgsquote unverhältnismäßig hohen Anteil für interne Aufklärungssysteme.

Studie von Verizon

dauerte, bis die Fehler behoben wurden (Bild 1). Entdeckt wurden diese Fälle vor allem durch Externe: in 26% der Fälle durch unbeteiligte Dritte, nur in 10% von Nutzers und die interne Auswertung von Log-Dateien, Fraud Detection, Incident Response und IT-Audits waren jeweils nur mit einem Prozent an der Aufklärungsquote beteiligt (Bild 2). Alle internen Verfahren scheinen systembedingt fehlerbehaftet zu sein. Umso wichtiger wird der Ansatz, unternehmensinterne Verfahren durch externe Prüfungen zu ergänzen, wie es ebenfalls im Entwurf der EU-Datenschutzgrundverordnung vorgesehen ist. Artikel 22 sieht zur Umsetzung der Pflichten des für die Verarbeitung Verantwortlichen vor, dass der für die Verarbeitung Verantwortliche „geeignete Verfahren zur Überprüfung der Wirksamkeit der in den Absätzen 1 und 2 genannten Maßnahmen“ einsetzt und ergänzend, dass die „Überprüfung von unabhängigen internen oder externen Prüfern durchgeführt“ wird.

Je nach Gefährdungslage und Komplexität der technischen Infrastruktur ist ein Information Security Management System (ISMS) erforderlich, um die Anforderungen des § 9 BDSG und damit auch des § 42 erfüllen zu können. Auch wenn nicht immer eine Zertifizierung nach DIN 27001 angemessen und erforderlich ist, so ist zumindest die Methode nach den vom Bundesamt für die Sicherheit in der Informationstechnik (BSI) herausgegebenen Grundschutzstandards für das Datenschutzkonzept in dem Baustein B 1.5 „Datenschutz“ sowie in der Maßnahme M 7.3 der Grundschutzkataloge generell zu empfehlen. Das Datenschutzkonzept ist als Pendant zum IT-Sicherheitskonzept notwendige Ergänzung der Informationssicherheit.

Informationspflicht

Ein weiterer Paradigmenwechsel korrigiert allzu ausufernde Auslegungen eines „unverhältnismäßigen Aufwandes“ durch die alternative Veröffentlichungspflicht in zwei deutschlandweit erscheinenden Tageszeitungen. Die Entschärfung des Entwurfes durch den Zusatz „oder durch eine andere, in ihrer Wirksamkeit hinsichtlich der Information der Betroffenen gleich geeignete Maßnahme“ auf Intervention des Bundesrates erfordert ebenfalls gleich wirksame alternative Informationswege, also zum Beispiel landesweit erscheinende Tageszeitungen bei regionalem Bezug. Auch dann bleibt es bei einem hohen Imagerisiko einer solchen Datenschutzverletzung für jedes betroffene Unternehmen.

Der Regelfall ist jedoch die Information der Betroffenen entweder auf elektronischem oder postalischem Weg. Ach hierbei ist der Inhalt durch die gesetzliche Regelung vorgegeben, um dem Betroffenen alle Informationen zur Vermeidung möglicher Nachteile zu geben.

Ein wirksames Datenschutzmanagement muss nach dem Prinzip „Folge dem Datum“ alle Prozesse im Unternehmen erheben, deren datenschutzrechtliche Zulässigkeit gewährleisten, die dem Stand der jeweiligen (Bedrohungs-) Technik erforderlichen Maßnahmen zum Schutz der zulässigerweise erhobenen Daten vor einem Missbrauch auch im Fall eines Versagens der Schutzmaßnahmen festlegen und deren Wirksamkeit prüfen können. Dabei muss sich jede verantwortliche Stelle dem Umstand stellen, dass interne Schutzmaßnahmen nur in der externen Widerspiegelung seine Wirksamkeit entfalten kann.

1 § 42a wurde eingefügt durch das Gesetz zur Regelung des Datenschutzaudits und zur Änderung datenschutzrechtlicher Vorschriften, Gesetzentwurf der Bundesregierung auf BT-Drs. 16/12011,

2 „Hat eine Daten verarbeitende Stelle Grund zur Annahme oder Kenntnis, dass unrichtige, unzulässig erhobene oder unzulässig gespeicherte personenbezogene Daten in der Weise genutzt wurden, dass dem Betroffenen daraus ein Nachteil entstanden ist oder zu entstehen droht, so hat sie diesen unverzüglich zu benachrichtigen.“

3 Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten nach § 42a Bundesdatenschutzgesetz (BDSG): Häufig gestellte Fragen (FAQs) erstellt vom Berliner Beauftragten für Datenschutz und Informationsfreiheit und freundlicherweise dem LDI NRW zur eigenen Veröffentlichung zur Verfügung gestellt unter: https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Technik/Inhalt/TechnikundOrganisation/Inhalt/Informationspflicht_bei_Datenpannen_____42a_BDSG_/Vorlage_FAQs_zur_Informationspflicht1.pdf

4 Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung) KOM (2012) 11

5 Data Breach Investigations Report 2013: http://www.verizonenterprise.com/DBIR/2013/

6 DBIR Industry Snapshot: Healthcare: http://www.verizonenterprise.com/resources/reports/rp_dbir-industry-snapshot-healthcare_en_xg.pdf

BigBrotherAwards 2013

http://www.bigbrotherawards.de/2013

Arbeitswelt: Apple Retail Germany GmbH

Der BigBrotherAward 2013 in der Kategorie Arbeitswelt geht an die Apple Retail Germany GmbH in München für die umfassende Videoüberwachung von Beschäftigten. Das Unternehmen betreibt die Apple Stores in Deutschland. In diesen sollen nicht nur Verkaufs- und Lagerräume flächendeckend und dauerhaft per Kamera überwacht worden sein, sondern auch Pausenräume. Diese Form der Totalkontrolle von Beschäftigten wäre in Deutschland rechtswidrig. Dabei zeigt sich die Firma uneinsichtig: Zum Beispiel wurden erst nach zähen Verhandlungen von Datenschutzbeauftragten die Hinweisschilder auf Videoüberwachung im Kundenbereich von Dackelaugenhöhe auf Hüfthöhe korrigiert.



Rena Tangens und Padeluun – Foto: Fabian Kurz

Globales Datensammeln: Google Inc.

In der Kategorie „Globales Datensammeln“ geht der BigBrotherAward an Google Inc., Mountain View, USA. Unter dem Deckmantel einer Suchmaschine und anderen Gratis-Diensten wie Maps, Docs und YouTube sammelt der Werbekonzern Google auf Schritt und Tritt Echtzeit-Daten über alles und jeden und kategorisiert Menschen für seinen Werbeprofit. Google missachtet europäisches Recht und nutzt seine marktbeherrschende Stellung, um die technokratische Ideologie eines allwissenden Supercomputers voranzutreiben, der besser weiß, was Menschen wollen als sie selbst.

Wirtschaft: Deutsche Post Adress GmbH und Co KG

Der BigBrotherAward 2013 in der Kategorie Wirtschaft geht an die Deutsche Post Adress GmbH und Co KG. In tausenden Postfilialen und im Internet geben jährlich Millionen Menschen in Deutschland Ihre Adress- und Umzugsdaten an. Diese bilden den Grundstock für die ständige Aktualität des Adressdatenbestands der Deutschen Post Adress GmbH. Und die verkauft ihre landesweite Ortskenntnis an zahlende Kunden weiter. Wer keinen Nachsendeantrag stellt, dem ist die Adressenrecherche der Preisträgerin trotzdem auf den Fersen, wenn es der werbenden Wirtschaft oder dem Forderungseinzug dient, notfalls sogar bis ans eigene Telefon.

Behörden & Verwaltung: Bundespolizei

Der BigBrotherAward 2013 in der Kategorie Behörden & Verwaltung geht an die Bundespolizei, vertreten durch ihren Präsidenten Dieter Romann, für Polizeikontrollen, bei denen Personen aufgrund ihres äußeren Erscheinungsbildes (Hautfarbe oder andere biologische Merkmale, ethnische Zugehörigkeit, nationale Herkunft, Religion, Sprache) gezielt aus einer Menschenmenge herausgegriffen werden, um ihre Personalien festzustellen und sie zu überprüfen. Diese verbreitete Praxis rassistischer Rasterungen nennt man „Racial“ oder „Ethnic Profiling“; auf verdächtiges Verhalten oder objektive Indizien als Verdachtsmomente kommt es bei dieser Kontrollpraxis nicht an.

Politik: Ministerpräsidenten der deutschen Bundesländer

Der BigBrotherAward in der Kategorie Politik geht an die Ministerpräsidenten der 16 deutschen Bundesländer für die Einrichtung des Gemeinsamen Beitragsservice von ARD, ZDF und Deutschlandradio als Nachfolger der GEZ. Seit Anfang Januar sind Rundfunkbeiträge nicht mehr für Geräte, sondern pro Wohnung zu entrichten. Dabei haben die Autoren des Rundfunkbeitragsstaatsvertrages die Chance verpasst, eindeutige, personenunabhängige Regelungen zu entwickeln. In der mehrjährigen Übergangsphase verarbeitet der neue Beitragsservice sogar viel mehr Daten als zuvor die GEZ. Die rechtliche Grundlage der Datenverarbeitung ist für Juristen zumindest zweifelhaft.

Tadelnde Erwähnungen:

Bundesanstalt für Finanzdienstleistungsaufsicht

Die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) führt seit dem 1. November 2012 ein zentrales „Beraterregister“. Dort werden alle Informationen über Beschwerden gesammelt, die es über Anlageberater gibt. Ob die Beschwerden berechtigt sind oder nicht, ist für die Erfassung unerheblich. Hält die BaFin Beschwerden für berechtigt, kann sie den Beschäftigten die Anlageberatung für bis zu zwei Jahre untersagen. Für die Betroffenen ist dies faktisch ein Berufsverbot und hat wahrschein-

lich auch arbeitsrechtliche Konsequenzen. Der Druck von Arbeitgebern und Vertriebsleitern, der Ursache für viele Fehler und Beschwerden ist, wird im Beraterregister nicht berücksichtigt Die Volksbank in Göppingen hat Verfassungsbeschwerde gegen das Beraterregister eingelegt.

Bundesregierung – Telekommunikationsbestandsdatenauskunft

Das Bundesverfassungsgericht hatte eine Neuregelung der „Änderung des Telekommunikationsgesetzes" und der „Bestandsdatenauskunft" gefordert, aber der neue Gesetzentwurf entspricht in vielen Punkten nicht den Anforderungen des Gerichts. Unter anderem soll die Identifizierung von Internetnutzerinnen und -nutzern über die IP-Adresse schon zur Ermittlung geringfügiger Ordnungswidrigkeiten sogar ohne konkrete Verdachtsmomente abrufbar sein .

Landkreis Peine

Der Landkreis Peine hat einem 24-jährigen Autofahrer angedroht, dass dieser zu einer medizinisch-psychologischen Untersuchung (MPU) müsse. Besagter Autofahrer hatte sich auf Facebook kritisch über fest installierte Radaranlagen an einer Landstraße geäußert. Hieraus leitet der Landkreis Peine ein „gewisses Maß an Konfliktpotential" ab, welches im Straßenverkehr nicht angebracht sei. Nachdem der Vorfall öffentlich wurde, räumte der Sprecher des Landkreises zwar eine Überreaktion eines Mitarbeiters ein. Gleichzeitig bestätigte er aber, dass der Landkreis in drei anderen Fällen Strafanzeigen wegen Internet-Einträgen mit grob beleidigendem Charakter gestellt habe.

EU-Überwachungssystem EUROSUR

„Eurosur" ist ein „Frühwarnsystem", das die „Überwachung, Ermittlung, Identifizierung, Nachverfolgung, Vorbeugung und das Abfangen" von illegalen Grenzübertritten in die EU erleichtern soll. Mit dem Einsatz von Drohnen, Satelliten, Radarüberwachung und auch von geheimdienstlichen Mitteln zur Vorfeldaufklärung wird die EU an ihren Außengrenzen weiter zu einer elektronischen Festung ausgebaut, um Migranten und Flüchtlinge abzuwehren. Damit wird das ohnehin schon eingeschränkte Asylrecht noch stärker ausgehöhlt. Der Innenausschuss des Europaparlaments hat „Eurosur" im November 2012 beschlossen.

Regis24 u.a.

Die Firma Regis24 und andere sogenannte Adressmittler bauen Datenbanken auf, die einem parallelen Zentral-Melderegister gefährlich nahe kommen – mit fragwürdigem Rechtsverständnis. Regis24 bietet Unternehmen den Service an, für sie Auskünfte im Melderegister einzuholen. Regis24 bringt die Daten in Erfahrung, um sie anschließend z. B. an die Bank weiter zu geben. Regis24 speicherte die Daten auch in den eigenen Datenbanken ab, um sie für weitere Anfragen zu nutzen. So legte Regis24 Stück für Stück und ohne Wissen der Betroffenen ein Schattenmelderegister an, das für Bürger und Bürgerinnen weder einsehbar, noch kontrollierbar ist.

Deutscher Musikrat GmbH

Der Deutsche Musikrat veranstaltet den renommierten Wettbewerb „Jugend musiziert". Für die Teilnahme ist es erforderlich, dass bei der Anmeldung sehr umfangreiche personenbezogene Daten angegeben und zur weitgehenden Verwendung freigegeben werden. Einige dieser Daten mögen zwar für die Durchführung des Wettbewerbs erforderlich sein, aber eine Veröffentlichung von Name, Vorname und Jahrgang, auch noch Geschlecht, vollständiges Geburtsdatum, Telefon- und Mobilnummer der zumeist minderjährigen Teilnehmenden im Internet ist nicht nachvollziehbar.

Palm WebOS

Palm vertreibt als Tochterfirma von Hewlett-Packard handelsübliche Smartphones, basierend auf HP's Betriebssystem WebOS. In den allgemeinen Geschäftsbedingen von Palm WebOS steht nicht nur, dass regelmäßig sensible Informationen zu Kontakten und Kalender an Palm übertragen werden. Auch dürfen Informationen wie Registrierungsdaten, Konto- und Geräteinformationen, Inhalte und technische Daten gespeichert, veröffentlicht, übertragen oder anderweitig verwendet werden.

Polizei Frankfurt (Oder), Mordkommission

Im Fall einer Entführung hat sie sachdienliche Hinweise aus der Bevölkerung über eine Web.de-E-Mail-Adresse entgegengenommen. Damit hat sie die Hoheit über die eingehenden Informationen (Hinweise, Mutmaßungen, Verdachtsmomente usw.) in private Hand gegeben. Normalerweise erfordern solche Ermittlungen großes Fingerspitzengefühl und höchste Professionalität, um Mutmaßungen nicht zu früh öffentlich werden zu lassen oder Zeugen zu gefährden. Eine Web.de-Adresse anmelden kann jedoch jeder – auch der Täter.

Rena Tangens

Dämpfer für die Arroganz von Apple

Verbraucher haben Rechte – und die gelten auch gegenüber Firmen, die sich pro forma in der Steuer- und Datenschutzvermeidungsoase Irland angesiedelt haben. Ein erfreuliches Urteil des Berliner Landgerichtes.

Die BigBrotherAwards hatten Apple bereits 2011 wegen seiner Datenschutzbestimmungen einen der ungeliebten „Oscars für Datenkraken" verpasst und die „Geiselnahme der Kunden mittels teurer Hardware" gerügt. Der vzbv (Verbraucherzentrale Bundesverband) prüfte 2012 die Allgemeinen Geschäftsbedingungen des Apple App-Stores. Insge-

samt 15 Punkte bemängelte der vzbv, die die Kunden unangemessen benachteiligten. Da der Konzern sich nur bedingt einsichtig zeigte, musste die Sache vor dem Landgericht Berlin geklärt werden. Das gab jetzt den Verbraucherschützern in vollem Umfang recht.

Die vom Gericht kassierten Vertragsklauseln sind schlicht eine Frechheit. Nicht nur sollen die Kunden eine globale Einwilligung zur Datenverarbeitung geben ohne zu wissen, für welche Zwecke. Sondern sie sollten auch gleich zustimmen, dass Apple die Daten ihrer Kontakte erhebt – ohne dass diese selbst dazu gefragt würden. Zusammenführung mit Informationen aus anderen Quellen, Datenweitergabe zu Werbezwecken an strategische Partner und Nutzung der Standortdaten der Kunden wollte sich Apple ebenfalls einräumen. Uns so weiter und so fort. Das alles auf 21 DIN A 4 Seiten. Was übrigens sich auf 117 Seiten erhöht, wenn die Kunden die AGB / Datenschutzbestimmung auf dem Display ihres iphones lesen wollen. Hier zeigt sich die maßlose Arroganz zu meinen, alles tun zu können, was dem Profit dient. Für die Kundinnen und Kunden gilt „friß oder stirb“.

In den Jura-Fakultäten von US-Universitäten wird durchaus gelehrt, was in Europa erlaubt ist und was nicht. Doch mit einem Augenzwinkern wird dort schon den Studierenden vermittelt, dass die Regeln nicht ernst zu nehmen seien, da ihre Einhaltung selten verfolgt würde und wenn, sei die zu erwartende Strafe ja locker aus der Portokasse zu bezahlen.

Die europäische Datenschutzgrundverordnung war angetreten, das zu ändern. Eine drohende Strafe bei Datenschutzverstößen von 2% vom Umsatz eines global tätigen Unternehmens ist dazu angetan, Datenschutz zur Chefsache zu machen. Die Reaktion der US-Unternehmen ist bekannt: Sie haben scharenweise Lobbyisten nach Berlin und Brüssel geschickt, um die geplante Datenschutzverordnung so lange mit Änderungsvorschlägen zu verwässern, bis sie gar nicht mehr für sie zutrifft. Dem müssen unsere Minister im EU-Ministerrat und die Europaabgeordneten endlich etwas entgegensetzen.

Kennen Sie den netten Witz aus der Netz-Frühzeit, in der Computer-Betriebssysteme (DOS, Windows, Mac, Unix etc.) mit Fluglinien verglichen wurden? Windows sieht nett aus, stürzt aber unvermittelt ab, bei Unix müssen die Fluggäste beim Bau des Flugzeugs selber mit anfassen. Bei der Apple Airline sehen alle Angestellten gleich aus, egal ob Bodenpersonal, Pilot oder Steward – man weiss nie, wen man gerade vor sich hat. Und wenn Sie bei Apple eine Frage haben, wie was funktioniert, dann klopft man Ihnen auf die Finger und sagt „Das brauchen Sie nicht wissen, das wollen Sie auch gar nicht wissen – und jetzt gehen Sie zurück an Ihren Platz und schauen einen Film.“ Die Grenze zwischen Nutzerfreundlichkeit und Bevormundung durch Technik ist bei Apple seit langem überschritten.

So erscheint einem das Logo dieser Firma mit den smarten Gadgets nicht als die Frucht vom Baum der Erkenntnis, sondern eher als der vergiftete Apfel, der Schneewittchen von der bösen Königin untergejubelt wurde. Nein, wir wollen nicht jedes Mal vor dem In-den-Apfel-Beißen das Kleingedruckte lesen. Sondern wir erwarten zu Recht, dass Obst mit Risiken und Nebenwirkungen aus dem Verkehr gezogen wird.

Das Urteil ist auf S. 79 nachzulesen.

Buchbesprechung



Dr. Martin Bahr:
Recht des Adresshandels
Erich Schmidt Verlag, 2011, 255 Seiten, ISBN 978-3-503-13060-3, 36,80 €

(wh) 2009 wurden im Bundesdatenschutzgesetz die Regelungen zum Adresshandel geändert. Auch wenn die neuen Regelungen zu keinen Einschränkungen im Adresshandel führten, sondern nur erweiterte Informations- und Auskunftspflichten für die Adresshändler und Einkäufer von Adressen einführten, führten die Änderungen zu einer gewissen Verunsicherung in der Branche. Hier setzt das Buch von Rechtsanwalt Dr. Martin Bahr an. Die Vorbemerkung darf getrost überblättert werden, dort finden sich solch gewagte Aussagen wie z.B. dass die Daten des Adresshändlers die Eigentumsgarantie des Art. 14 GG genießen würden. Unberücksichtigt bleibt, dass dies für personenbezogene Daten nur sehr bedingt – wenn überhaupt – gilt. Die Darstellung der konkreten Rechtslage für den Handel mit Adressdaten ist dagegen gut aufbereitet und mit diversen Beispielen und Praxistipps erläutert. Dadurch ist es nicht nur Unternehmen möglich, sich im Bereich Adresshandel möglichst rechtssicher zu verhalten. Auch Verbraucher/innen und Verbraucherschützer erhalten eine guten Überblick über rechtlich zulässige und unzulässige Verhaltensweisen. Noch besser wäre das Buch allerdings, wenn der Autor auf seine lobbyistisch gefärbten politischen Aussagen verzichtet und sich auf die rechtliche Darstellung beschränkt hätte.

Fazit: Unter der Berücksichtigung, dass dieses Buch aus Sicht eines „seit Jahren im gewerblichen Adresshandels tätigen“ Anwalts geschrieben wurde, stellt dieses Werk eine sehr anschauliche und ausführliche Darstellung des Rechts im Adresshandel dar, die auch zwei Jahr nach erscheinen aktuell ist.

Datenschutznachrichten

Datenschutznachrichten aus Deutschland

Bund

Erste deutsche Verhaltensregeln nach § 38a BDSG bei der Versicherungswirtschaft

Der Gesamtverband der Deutschen Versicherungswirtschaft (GDV) hat die am 02.11.2012 vom Berliner Beauftragten für Datenschutz und Informationsfreiheit (BlnBDI) anerkannten Verhaltensregeln für die Datenverarbeitung in der Versicherungsbranche veröffentlicht. Der GDV ist damit der erste Verband in Deutschland, der erfolgreich der zuständigen Aufsichtsbehörde seine Verhaltensregeln nach § 38a BDSG vorgelegt hat. Vorausgegangen waren dieser Anerkennung langwierige Verhandlungen des GDV mit der AG Versicherungswirtschaft des Düsseldorfer Kreises (DK), dem Zusammenschluss der deutschen Datenschutzaufsichtsbehörden. An den Verhandlungen waren auch Vertreter von Versicherungsunternehmen und teilweise der Verbraucherzentrale Bundesverband (vzbv) beteiligt.

Der Vorsitzende der GDV-Hauptgeschäftsführung Jörg von Fürstenwerth freute sich: „Der Schutz von Kundendaten hat für uns oberste Priorität. Die neue Selbstverpflichtung konkretisiert erstmals die allgemeinen Regeln des Bundesdatenschutzgesetzes für die Versicherungswirtschaft und schafft Transparenz über die Datenverarbeitung in unserer Branche. So wollen wir das Vertrauen unserer Kunden in unternehmensinterne Abläufe weiter stärken. Die neue Selbstverpflichtung dokumentiert das gemeinsame Verständnis von Versicherungswirtschaft, Daten- und Verbraucherschützern über die Datenschutzregeln für Versicherungen.“ Der Dialog mit den Daten- und den Verbraucherschützern solle über die aktuelle Selbstverpflichtung hinaus fortgesetzt werden, um weitere gemeinsame Antworten auf noch offene Datenschutzfragen zu finden. Der BlnBDI Alexander Dix hofft, dass andere Branchenverbände dem Beispiel des GDV folgen: „Von den Datenschutzbehörden geprüfte Selbstverpflichtungen sind ein sinnvoller Weg, allgemeine Datenschutzregeln branchenspezifisch auszufüllen. Dies wird auch im Kontext der künftigen Europäischen Datenschutz-Grundverordnung eine wichtige Rolle spielen.“

Die Verhaltensregeln, denen die Versicherungsunternehmen einzeln beitreten müssen, enthalten ein umfangreiches Normenwerk mit 31 Artikeln. Von den Unternehmen wird u. a. Folgendes abverlangt:

- Sie schreiben ein umfassendes Daten-schutz- und Datensicherheitskonzept vor. Darin werden die technischen und organisatorischen Maßnahmen beschrieben, die das Unternehmen zum Schutz der Daten getroffen hat.
- Sie dokumentieren wichtige Datenverarbeitungsvorgänge und machen so ihren Umgang mit personenbezogenen Daten für die Datenschutzbehörden besser überprüfbar.
- Sie informieren ihre Kunden über alle wichtigen Aspekte der Datenverarbeitung. So müssen zum Beispiel Dienstleister, die für ein Unternehmen personenbezogene Daten verarbeiten, namentlich oder ihrer Berufsgruppe nach in einer Liste aufgeführt werden. Jeder Kunde kann die Liste im Internet einsehen oder sich zuschicken lassen.

Die Unternehmen müssen in einer Frist von maximal drei Jahren ab Beitritt ihre Datenverarbeitung den neuen Anforderungen anpassen. Die Unternehmen, die sich zur Einhaltung der definierten Verhaltensregeln verpflichtet haben, werden demnächst auf der GDV-Homepage veröffentlicht. Die Verhaltensregeln finden sich im Internet unter http://www.gdv.de/wp-content/uploads/2013/03/GDV_Code-of-Conduct_Datenschutz_2012.pdf (GDV, PE v. 27.03.2013, Versicherungswirtschaft und Datenschützer schaffen neue Maßstäbe für Datenschutz; ULD, 34. Tätigkeitsbericht, Kap. 5.1.3).

Bund

Videoeinsatz gegen Extremisten

Aus einer Antwort des Bundesinnenministeriums (BMI) auf eine Kleine Anfrage der Linksfraktion im Bundestag geht hervor, dass das Bundesamt für Verfassungsschutz (BfV) seit den Terroranschlägen vom 11.09.2001 insgesamt 962 Personen aus dem islamistischen Milieu per Video überwacht hat. Aktuell würden vom BfV 20 mutmaßliche Islamisten sowie Rechtsextremisten mittels Kamera ausgespäht. Das Bundeskriminalamt hat danach in den vergangenen 12 Jahren 84 Personen per Video überwacht, um terroristische Straftaten zu verhindern oder aufzudecken; es fanden April 2013 drei derartige Maßnahmen statt. Das BMI bestreitet, dass in seinem Zuständigkeitsbereich Verdächtige mit Anlagen überwacht werden, die biometrische Merkmale oder Verhaltensmuster von Menschen erfassen können. Der Antwort ist aber eine Liste beigefügt, wonach Behörden, Unternehmen und Wissenschaft an mindestens sechs Projekten zu Biometrie und Verhaltensmustererkennung forschen, was mit mehr als 13 Millionen Euro staatlich gefördert wird. Der Kommentar des Linkspartei-Abgeordneten Jan Korte: „Ich bin gespannt, wann Bundesinnenminister Hans-Peter Friedrich erklärt: Niemand hat die Absicht, derartige Videoüberwachungsanlagen zu errichten“ (Der Spiegel 17/2013, 16; BT-Drs. 17/12704).

Bund

Bahn nutzt Bonusdaten für Werbezwecke

Die Deutsche Bahn will mit Daten ihrer Reisenden in Zukunft Geld verdienen: Informationen von VielfahrerInnen sollen für die Werbung anderer Unternehmen genutzt werden. Zu diesem Zweck lässt sie sich seit Anfang 2013 neue Vertragsbedingungen von solchen BahnCard-InhaberInnen bestätigen, die auch Bahn-Bonus-KundInnen sind. Künftig sollen diese auf ihre „individuellen Bedürfnisse“ zugeschnittene Werbeangebote erhalten - von Kooperationspartnern wie Banken, Versicherungen oder Fast-Food-Ketten.

Die Daten, die die Bahn für ihre passgenaue Werbung erhebt, sind der Preis der Fahrkarte, Abgangs- und Zielbahnhof, die Wagenklasse und die Verkaufsstelle. Der für die Bahn zunächst für zuständig angesehene Berliner Datenschutzbeauftragte Alexander Dix sagte zu, den Vorgang zu prüfen: „Hier scheint die Bahn ihre Interessen über die schutzwürdigen Interessen ihrer Kunden zu stellen.“ Thilo Weichert, Datenschutzbeauftragter in Schleswig-Holstein, prognostizierte: „Die Teilnahme an dem Programm darf nicht davon abhängig gemacht werden, ob ich der Werbenutzung zustimme oder nicht. Die Bahn wird sich damit eine blutige Nase holen.“

Die Bahn wies die Darstellung der Presse zurück. Die Bahn betreibe „keinen Datenhandel“, sagte zwar die Bahn-Datenschutzchefin Chris Newiger. Und in einer Presseerklärung heißt es: „Die DB gibt bislang keinerlei Kundendaten zu Marketingzwecken an Dritte weiter und plant dies auch künftig nicht.“ Daten von Bahn-Bonus-Kunden könnten auch zu Marketingzwecken genutzt werden, dieser Nutzung könnten die Kunden aber „selbstverständlich“ widersprechen. Das Bahn-Bonus-Programm entspreche „voll und ganz“ dem Bundesdatenschutzgesetz (BDSG), erklärte der Konzern in einer Pressemitteilung. Damit machte die Bahn offensichtlich auch schon ihre Kehrtwende. Im Infoblatt oder sonstigen Hinweisen der Bahn ist vom Widerspruchsrecht keine Rede.

In Antwortschreiben an Betroffenen, die der Werbenutzung nach § 28 Abs. 4 BDSG widersprachen, teilte kurz vorher der Bahnbonus-Service noch mit: „Die Änderung der bahn.bonus-Bedingungen war notwendig, um Ihnen auch weiterhin auf Ihre individuellen Bedürfnisse ausgerichtete Angebote und Vorteile unterbreiten zu können. Das bedeutet, dass wir Ihre personenbezogenen Reisedaten, die durch das Punktesammeln gespeichert werden, für Marketingzwecke nutzen dürfen. Sollten Sie sich vom bahn.bonus-Programm abmelden, werden sämtliche bisher von Ihnen gesammelten Prämien- und Statuspunkte gelöscht und es können keine neuen Prämien- und Statuspunkte gesammelt werden. Wir bitten Sie um Verständnis, dass wir Ihnen diese - auf Ihren Wunsch - gelöschten Punkte nicht wieder gutschreiben können.“ Die Prüfung des Vorgangs ergab, dass hierfür die DB Fernverkehr AG mit Sitz in Frankfurt verantwortlich ist, weshalb der Hessische Datenschutzbeauftragte (HDSB) letztlich bekannt gab, die Bahn habe zunächst „nicht hinreichend klar kommuniziert“, dass ein Widerspruch gegen die Verwendung der Daten für Werbezwecke jederzeit möglich sei. Die DB Fernverkehr AG habe auf Anregung des HDSB „die Transparenz für die Kunden inzwischen hergestellt“. Die neuen Bedingungen für das Bonus-Programm sollen ab Dezember 2013 auch tatsächlich umgesetzt werden.

Zweimal erhielt der Bahn-Konzern schon einen Big-Brother-Award. Bereits im ersten Jahr der Preisverleihung im Jahr 2000 war die Bahn negativ aufgefallen und prämiert worden für ihre flächendeckende Videoüberwachung auf Bahnhöfen (DANA 4/2000, 9f.). Sieben Jahre später hatte der Konzern seine BahnCard-KundInnen verpflichtet, ein Foto zu liefern und ihr Geburtsdatum anzugeben. In die BahnCard 100 war ohne Wissen ihrer Inhabenden ein RFID-Chip eingebaut worden (DANA 4/2007, 164ff.), worauf die Bahn inzwischen immerhin hinweist (Klawitter, Der Spiegel 12/2013, 74; Öchsner, Bahn will mit Kunden-Daten Geld verdienen, SZ 18.03.2013, 1; Stüben, Bahn will Kundendaten nutzen, KN 19.03.2013, 11; PM HDSB 04.04.2013, Kundendatenverarbeitung beim Bahn-Bonus-Programm der Deutschen Bahn ist datenschutzkonform).

Bund

BMI kauf Quellen-TKÜ-Software

Das Beschaffungsamt des Bundesministeriums des Innern (BMI) hat nach Presseangaben für 147.000 Euro Software zur Durchführung von Abhörmaßnahmen bei der Internet-Telefonie (Quellen-TKÜ) eingekauft. Das Amt hat demgemäß eine Lizenz für zehn Computer von Firma Elaman/Gamma mit Sitz in München erworben. BMI und das Bundeskriminalamt (BKA) bestätigten die Transaktion. Derweil meint der Generalbundesanwalt Harald Range, dass derzeit keine ausreichende Rechtsgrundlage für den Einsatz einer solchen Software vorliegt.

Der Einkauf der Elaman-Software soll die Zeit überbrücken, in der eine vom BKA selbst entwickelte Software nach einem aufwändigen Qualitätssicherungsprozess (QSP) zum Einsatz bei der Überwachung von Internet-Telefonaten gelangen kann. Diese Software soll nicht vor Ende 2014 verfügbar sein. Die Software der umstrittenen Münchener Firma wird von Beratern der Firma CSC geprüft. Ein vorzeitiger Kauf einer Lizenz für zehn Computer deutet auf aktuelle Überwachungsmaßnahmen hin, bei denen das BKA offenbar Eile hatte, den Mitschnitt von Internet-Telefonaten durchzuführen (Borchers, Innenministerium kauft Software für Quellen-TKÜ, www.heise.de 02.05.2013).

Bund

Anträge auf Stasi-Akteneinsicht nehmen weiter zu

Der Bundesbeauftragte für die Stasi-Unterlagen Roland Jahn erklärte anlässlich der Vorstellung seines 11. Tätigkeitsberichtes am 12.03.2013, dass im Jahr 2012 die Anträge auf persönliche Einsicht in Stasi-Papiere auf 88.231 gestiegen sind. Dies waren ca. 7.200 Anträge mehr als 2011. 10% der Erstanträge kommen von Familienangehörigen Verstorbener. Jahn meinte, es gebe heute ein steigendes Interesse einer neuen Generation, die frische

Fragen stelle. So wollten erwachsene Kinder wissen, weshalb Eltern mitgemacht oder sich angepasst hätten und welche Lehren in dieser Vergangenheit stecken (vgl. DANA 1/2011, 16; 11. Tätigkeitsbericht, BT-Drs. 17/12600; SZ 13.03.2013, 6; http://www.bstu.bund.de 12.03.2013).

Bund

AfD-Wahl- und Spendenwerbung mit fremden Daten

Die neue Anti-Europa-Partei „Alternative für Deutschland" (AfD) hat zur Finanzierung ihres Wahlkampfes zur Bundestagswahl 2013 einen „Arbeitskreis Fundraising" eingerichtet, der mit Mailing-Aktionen Spenden aquiriert. AfD-Schatzmeister Norbert Stenzel: „Als Mitglied im CDU-Wirtschaftsrat habe ich ein dickes Verzeichnis mit Mitgliederadressen." Diese sollen genutzt werden. Unionsfraktionsvize und Präsidiumsmitglied im CDU-Wirtschaftsrat Michael Fuchs empörte sich über diesen „Datendiebstahl": „Kein Mitglied darf Daten für private Zwecke nutzen, schon gar nicht für eine andere Partei." Die AfD will auch ihre Kontakte in Arbeitgeberverbänden und Industrie- und Handelskammern (IHK) nutzen. Stenzel kündigte an, die internen Wahllisten für die Vollversammlungen der IHK auszuwerten. Ein Sprecher des Industrie- und Handelskammertages warnte, man werde konkreten Hinweisen auf Datenmissbrauch nachgehen. Im April 2013 hatte die AfD schon 600.000 Euro an Geldern beschafft (Der Spiegel 17/2013, 13).

Bayern

Innenminister will mehr Videokontrolle im ÖPNV

Der bayerische Innenminister Joachim Herrmann (CSU) fordert eine flächendeckende Videoüberwachung des öffentlichen Nahverkehrs in allen Großstädten: „Die Fahrgäste erwarten ein hohes Maß an Sicherheit." Als Vorbild nannte Herrmann die Landeshauptstadt München, in der die öffentlichen Verkehrsmittel am umfangreichsten mit Kameras ausgestattet seien. In München seien kaum noch S-Bahnen ohne Videokameras im Einsatz. Als Negativ-Beispiele nannte er die Städte Augsburg, Regensburg, Ingolstadt, Fürth und Erlangen, in denen nicht einmal in den Hauptbahnhöfen Kameras installiert seien. Für diese Versäumnisse machte er die Bahn verantwortlich, von der er mehr Engagement einforderte.

In den vergangenen fünf Jahren ist die Videoüberwachung im Freistaat stark ausgeweitet worden, insbesondere im öffentliche Personennahverkehr (ÖPNV). Nach Ansicht von Innenminister Herrmann trägt die Videoüberwachung dazu bei, die BürgerInnen besser vor Kriminalität zu schützen und ihr „subjektives Sicherheitsgefühl" zu stärken. „Die Videoüberwachung schreckt potenzielle Täter ab, verbessert und beschleunigt nötige Hilfe und erleichtert Ermittlungen." Schon nach dem tödlichen Angriff auf Dominik Brunner im Jahr 2009 auf dem Münchner S-Bahnhof Solln verlangte Herrmann die „lückenlose Überwachung". In Folge haben Freistaat und Verkehrsbetriebe Millionen mit unterschiedlichem Erfolg in die Überwachungsanlagen des Nahverkehrs investiert. Von den insgesamt 148 S-Bahnhöfen im Raum München sind bislang nur 18 mit Kameras ausgerüstet. Die Züge dagegen sind nahezu komplett mit Videokameras ausgestattet, die das Geschehen aufzeichnen. Die U-Bahnhöfe sind komplett überwacht, in 108 der 576 Züge hängen Kameras. In Nürnberg und Fürth wird die U-Bahn komplett überwacht, von den 22 S-Bahnhöfen sind lediglich zwei mit Videotechnik ausgestattet. Von den etwa 1.200 Bussen, die in Bayerns Großstädten fahren, ist nicht einmal ein Drittel videoüberwacht. Herrmann empfiehlt den Kommunen, bei Neuanschaffungen künftig Videoanlagen mitzubestellen.

Hermann forderte zudem von der Deutschen Bahn, mehr Geld in die Sicherheit der Bahnhöfe zu investieren. Der versuchte Bombenanschlag auf den Bonner Hauptbahnhof im Dezember 2012 habe gezeigt, dass man im öffentlichen Nahverkehr „jederzeit mit Terrorakten" rechnen müsse. Zwar waren in Bonn Kameras installiert, jedoch keine Aufzeichnungen gemacht worden. Herrmann nannte dies unbefriedigend. „Ich erwarte von der Bahn, dass eine Aufzeichnung in der Größenordnung von 72 Stunden stattfindet." Als Beleg für den Erfolg der Videoüberwachung führte Herrmann rückläufige Kriminalitätszahlen in München an. So sei die Zahl der Straftaten im Nahverkehr in den vergangenen zehn Jahren um fast 30% auf etwa 10.000 Delikte gesunken. Auch die Gewalt nahm ab; die Zahl der Vorfälle sank um 14%. Bayernweit registrierte die Polizei im Nahverkehr 2012 knapp 15.000 Straftaten, 27% weniger als noch 2002. Welchen Beitrag die Videoüberwachung dazu tatsächlich geleistet hat, ist unklar. Im Februar 2013 sah sich das Innenministerium auf eine Anfrage der Grünen nicht in der Lage, eine statistisch belegbare Aussage darüber zu treffen, ob eine „Videoüberwachung kausal für die Aufklärung bzw. Verhinderung einer Straftat oder ermittlungsunterstützend war". Polizei und Sicherheitsdienste haben in den vergangenen Jahren ihre Einsätze in Bussen, Tram-, U- und S-Bahnen deutlich verstärkt. Münchens Polizei-Vizepräsident Robert Kopp erklärte: „Das Sicherheitskonzept funktioniert sehr gut." Die Videoüberwachung sei dann besonders hilfreich, wenn es darum gehe, Straftäter zu ermitteln.

Kritik an Herrmanns Vorstoß kam vom Bayerischen Landesbeauftragten für Datenschutz Thomas Petri: „Ich halte eine flächendeckende Überwachung des öffentlichen Nahverkehrs für bedenklich. Diese Politik mag vor dem Hintergrund diverser öffentlichkeitswirksamer Straftaten verständlich sein." Er bezweifelt aber, ob ein solcher Eingriff wirklich erforderlich ist. Auch die Grünen im Bayerischen Landtag halten den neuerlichen Vorstoß des Innenministers für überzogen, so die innenpolitische Sprecherin der Grünen, Susanna Tausendfreund: „An Brennpunkten sind Kameras samt Aufzeichnung ja gegebenenfalls noch vertretbar, aber doch nicht flächendeckend in allen Zügen, jedem Bus, jeder Tram und an jeder Haltestelle." Die SPD wirft Herrmann dagegen vor, zu lange untätig gewesen zu sein. SPD-Fraktionschef Markus Rinderspacher sagte: „Am Abend werden die Faulen fleißig." Der Ausbau der Videoüberwachung im Nahverkehr hätte längst weiter fortgeschritten sein

können. Laut einem Regierungsbericht sind im Freistaat 17.000 Kameras bei öffentlichen Stellen im Einsatz. Ob an Schulen, Wertstoffhöfen, Mehrgenerationenhäusern oder in Bussen - es gibt kaum noch unbeobachtete Orte des öffentlichen Lebens (Szymanski, Mehr Videoüberwachung in den Zügen, SZ 04.04.2013, 40).

Berlin

CDU-Plattform beschaffte unzulässig Werbedaten

Eine Mitmach-Kampagne der CDU im Internet („Was mir am Herzen liegt“) verstieß nach Ansicht von Datenschützern gegen das Datenschutzgesetz. Auf der Website Regierungsprogramm.CDU.de wurden Parteimitglieder und BürgerInnen bis Ende April 2013 aufgerufen, am Regierungsprogramm mitzuschreiben. Wie bei Online-Umfragen üblich gibt es auf der Seite eine Erklärung, über die die UserIn in die Speicherung ihrer Daten einwilligt. Das Einverständnis zur Datenspeicherung war gekoppelt an das Einverständnis, Werbematerial der Partei zu akzeptieren: „Ich bin mit der Erhebung, Speicherung und Nutzung der vorstehenden personenbezogenen Daten sowie der besonderen Daten (§ 3 Abs. 9 BDSG z. B. politische Meinungen) einverstanden. Die Daten werden von der CDU Deutschlands, ihren Gliederungen, Vereinigungen und Sonderorganisationen für die Übersendung von Einladungen und Informationsmaterial - auch per E-Mail - genutzt. Eine sonstige Weitergabe an Dritte findet nicht statt. Dieses Einverständnis kann jederzeit mit Wirkung für die Zukunft widerrufen werden.“

Aus Sicht von Datenschützern ist die Datenspeicherung für Werbezwecke nicht in Ordnung, so z. B. der Datenschutzbeauftragte von Schleswig-Holstein Thilo Weichert: „Im politischen Bereich ist ein solches Verfahren ungewöhnlich. Die Möglichkeit, einen Widerspruch gegen die Werbenutzung einzulegen, ist unbedingt gesetzlich garantiert. Es geht also nicht, dass erst mal das Akzeptieren einer Werbenutzung technisch erzwungen und danach die Möglichkeit zum Widerspruch eingeräumt wird. Aus datenschutzrechtlicher Sicht muss man das eine vom anderen trennen, damit der User mitmachen kann - aber trotzdem die Option hat, auf Werbematerial und Einladungen zu verzichten.“ Weicherts Kollege Alexander Dix, Beauftragter für Datenschutz und Informationsfreiheit in Berlin, kündigte eine Prüfung an: „Es wird auf den ersten Blick nicht ersichtlich, was mit den bereits eingegebenen Daten passiert, wenn der Nutzer die Einverständniserklärung ablehnt. Werden diese unverzüglich gelöscht - oder im Hintergrund auf dem Server gespeichert? Auch das gilt es aufzuklären.“ Zwar konnte jede UserIn die Datenschutzbestimmung einfach ablehnen. Tat Sie das, wurde sie jedoch mit einem Pop-up-Fenster aufgefordert, der Erklärung zuzustimmen. Nur dann war das Mitmachen möglich.

Der IT-Jurist Nikolaus Forgó meinte: „Hier wird die Einwilligung der Datenspeicherung mit dem Akzeptieren einer Werbenutzung verknüpft. Ein Widerspruch ist nur nachträglich möglich.“ Das verstoße gegen das sogenannte Kopplungsverbot. Demnach ist die Verknüpfung eines Vertragsabschlusses mit der Einwilligung der Datennutzung zu Werbezwecken weitestgehend unzulässig (§ 28 Abs. 3b BDSG). Zwar greife das Gesetz unmittelbar nur beim Abschluss eines Vertrags mit einem privaten Akteur. Das sei bei der Mitmachplattform, auf der Leute ihre politische Meinung abgeben und nichts käuflich erwerben, nicht der Fall. „Aber der Rechtsgedanke, der dahinter steht, ist klar: Eine Verknüpfung von beidem ist wohl rechtswidrig. Der User muss die Möglichkeit haben, Werbung abzulehnen und sich trotzdem politisch beteiligen zu können.“ Das hier angewendete Verfahren habe „mit Freiwilligkeit nichts mehr zu tun“. In der CDU-Parteizentrale sah man darin kein Problem und betonte, „Einladungen und Informationsmaterial“ seien nicht mit Parteiwerbung gleichzusetzen. „Bei der verwendeten Einverständniserklärung handelt es sich um eine Standard-Formulierung, die wir auf vielen unserer Parteiportale benutzen“. Man wolle „die Mitmachenden auch über den Fortgang der Aktion auf dem Laufenden“ halten. Die CDU-Zentrale ließ nach der Kritik in der Öffentlichkeit eine Kleinigkeit auf dem Portal anpassen: Der ursprüngliche Ja/Nein-Button zur Datenschutzerklärung wurde zu einem einzigen Button verschmolzen; die Erklärung tauchte direkt unter dem Feedback-Feld auf. Der Wortlaut blieb derselbe (Meiritz, Datenschützer kritisieren neue CDU-Plattform, www.spiegel.de 15.03.2013; Meiritz, Das Märchen von der Mitmach-CDU, www.spiegel.de 15.03.2013).

Hessen

Landespolizeidrohne im Einsatz

Aus einem Schreiben der hessischen Staatskanzlei an den Landtagsabgeordneten der Grünen Jürgen Frömmrich geht hervor, dass die Überwachungsdrohne der Landespolizei bisher in elf Fällen eingesetzt worden ist. Der Abgeordnete hatte sich 2012 mit Innenminister Boris Rhein (CDU) über die Frage gestritten, wie viele Informationen über das ferngesteuerte, einem kleinen Hubschrauber ähnelnde und mit einer Kamera ausgestattete Gerät die breite Öffentlichkeit bekommen dürfe. Der Innenminister hatte damals lediglich bestätigt, dass das Land Hessen im Jahr 2009 ein „unbemanntes Luftfahrtsystem“ zum Preis von rund 38.000 Euro angeschafft habe. Ähnliche Überwachungssysteme besitzen auch die Polizeikräfte in Berlin, Sachsen und Niedersachsen sowie die Bundespolizei. Angaben zu der Zahl und zur Art der bisherigen Einsätze wollte Rhein damals „aus einsatz- und ermittlungstaktischen Gründen“ nicht machen. Frömmrich hatte bezweifelt, dass Eingriffe in die Privatsphäre, wie sie mit Drohnen möglich seien, auf einer sicheren rechtlichen Grundlage geschähen.

Der Chef der Hessischen Staatskanzlei Axel Wintermeyer (CDU) hat jetzt eine Anfrage des Landtagsabgeordneten beantwortet und mitgeteilt, dass Hintergrund des Drohneneinsatzes in einem Fall ein Tötungsdelikt gewesen sei; bei den anderen Einsätzen sei es um Rockerkriminalität, Waffenhandel, Bandendiebstahl und Drogenhandel gegangen. Nach Wintermeyers Angaben diente das unbemannte Gerät in den genannten elf Fällen dazu, „potentielle Zielobjekte

polizeilicher Exekutivmaßnahmen“ und sogenannte Betäubungsmittelplantagen auszuspähen. Der Einsatz sei nur bei Spezialeinsätzen in besonderen Lagen erlaubt. Dazu zählten bestimmte Gefahrensituationen, Entdeckungsrisiken und schwer zugängliche Einsatzräume. Der frühere Landespolizeipräsident Norbert Nedela habe zuvor etwas anderes angekündigt, kommentierte Frömmrich. Darum habe er die Befürchtung gehabt, dass die Drohne auch bei Großveranstaltungen und Demonstrationen eingesetzt werde, wie dies in Niedersachsen der Fall gewesen sei. Trotz einer gewissen Beruhigung beklagte er, dass ein monatelanger Schriftwechsel nötig gewesen sei, um die nötige parlamentarische Kontrolle auszuüben (Hetrodt, Polizei-Drohne war elfmal im Einsatz, www.faz.net 27.03.2013).

Niedersachsen

Vorwurf der Mitarbeiterüberwachung beim ADAC

Die ehemalige IT-Leiterin im fünftgrößten der 18 deutschen ADAC-Gaue, Marion Wille, 40, gibt an, sie habe im Auftrag des dortigen ADAC-Geschäftsführers Hans-Henry Wieczorek und anderer Führungskräfte den E-Mail-Verkehr von MitarbeiterInnen und speziell von BetriebsrätInnen beim ADAC Niedersachsen/Sachsen-Anhalt ausspioniert. Ziel sei es gewesen, belastendes Material vor allem gegen die Arbeitnehmervertreter und Informationen über deren Arbeit zu finden und zu sammeln. Nachdem sich Wille im Februar 2013 dem Betriebsrat offenbart hatte, stellte dieser Strafanzeige. Die Staatsanwaltschaft Hannover sieht nach den Worten ihres Sprechers „einen begründeten Anfangsverdacht“ und hat ein Ermittlungsverfahren eingeleitet, das sich gegen den Geschäftsführer richte. Die Geschäftsführung des ADAC-Gaus erhielt einen Monat Zeit, auf die vom Betriebsrat vorgebrachten zahlreichen Vorwürfe zu reagieren. Sollten sich die Vorwürfe gegen die ADAC-Leitung bestätigen, drohen den Betroffenen bis zu einem Jahr Haft.

Klaus Kocks, Sprecher des ADAC-Gaus, wies die Spitzelvorwürfe zurück: „Eine Anweisung zur Ausforschung hat es seitens der Geschäftsführung zu keinem Zeitpunkt und in keiner Form gegeben. Das Ganze ist ein niederträchtiges Geflecht aus Halbwahrheiten und glatten Lügen.“ Der Autoclub werde sich zur Sache nicht äußern, bis das Ermittlungsverfahren abgeschlossen sei. Detaillierte Fragen der Presse ließen der ADAC Niedersachsen/Sachsen-Anhalt und sein Geschäftsführer deshalb unbeantwortet. Stattdessen warnte deren Anwalt, eine Berichterstattung über die Vorgänge wäre rechtswidrig. Die Spitzelvorwürfe sind auch Gegenstand arbeitsgerichtlicher Verfahren. Wille gibt an, nach einem ADAC-kritischen Artikel in einer Boulevardzeitung im April 2009 habe der Geschäftsführer sie beauftragt, den E-Mail-Verkehr von Mitarbeitern nach bestimmten Schlüsselwörtern zu durchforsten, um etwaige Informanten der Zeitung zu enttarnen. Aus vertraulichen Unterlagen geht ferner hervor, dass die IT-Chefin im September 2009 dafür sorgen sollte, dass E-Mails des damaligen Pressesprechers des ADAC-Gaus künftig automatisch und heimlich auch an die Geschäftsführung gingen.

Später, gibt Wille an, sei sie unter anderem vom Geschäftsführer angewiesen worden, die E-Mail-Korrespondenz des Betriebsrates zu bespitzeln: „Man wollte sehen, mit wem der Betriebsrat kommuniziert und was er vorhat.“ Sie bedauert ihr Verhalten und sagt, sie fühle sich von der Geschäftsführung „als Spitzel instrumentalisiert“. Stephan Korb, Anwalt von Wille sowie des Betriebsrates, erläuterte das Verhalten der IT-Leiterin: „Es wurde suggeriert, dass derjenige, der gegen den Betriebsrat vorgeht, eine gute Tat am ADAC begeht.“ Die Spitzel-Ermittlungen sind ein Höhepunkt in den jahrelangen Auseinandersetzungen beim ADAC Niedersachsen/Sachsen-Anhalt. Von der Geschäftsführung gebe es, so Anwalt Korb, „ständige Attacken, die wir als massive Behinderungen der Betriebsratsarbeit werten. Seit dem Amtsantritt von Geschäftsführer Wieczorek, eines früheren Managers beim Mitteldeutschen Rundfunk, gab es in fünf Jahren 92 arbeitsgerichtliche Auseinandersetzungen - bei etwa 140 Beschäftigten. Viele Mitarbeiter haben den Regionalclub verlassen, etliche davon unfreiwillig. Auch der seit Oktober 2011 erkrankten IT-Leiterin wurde nach ihren Spitzelvorwürfen gekündigt.

Aus den Reihen der ehrenamtlich Aktiven beim ADAC wurde Kritik laut. Burkhard Scheunert, bis Dezember 2011 sechs Jahre lang Vorstandsmitglied des Gaus Niedersachsen/Sachsen-Anhalt meinte: „Der Geschäftsführer macht, was er will, und der Vorstand macht alles mit, weil der Geschäftsführer ihn fest im Griff hat.“ Ex-IT-Leiterin Wille wirft dem Geschäftsführer außerdem vor, sie im Juni 2010 und im April 2011 in sein Wohnhaus bestellt zu haben, um sie privat für sich an seinem PC arbeiten zu lassen. Spitzelvorwürfe im ADAC gab es auch in der Vergangenheit. 2011 wurde bekannt, dass in der Nürnberger Zentrale des Gaus Nordbayern Abhöranlagen gefunden wurden, mit denen Büros und Sitzungsräume bespitzelt werden konnten. Wer diese angebracht hatte, blieb unklar (vgl. DANA 2/2011, 78f.; Ritzer, Ausspioniert, SZ 21.03.2013, S. 1/; Justiz ermittelt gegen ADAC Niedersachsen, www.rp-online.de 21.03.2013).

Niedersachsen

Anonyme Reinheitschecks für Drogen geplant

Nach Berlin und Schleswig-Holstein plant nun Niedersachsens Gesundheitsministerin Cornelia Rundt (SPD) das Angebot eines anonymen Drug-Checks. SPD und Grüne hatten im Februar 2013 im Koalitionsvertrag ein Modellprojekt angekündigt. Zunächst soll gemäß einer Ministeriumssprecherin geprüft werden, wie das Projekt juristisch sauber umgesetzt werden kann. Zum Zeitplan und den Einzelheiten könne sie daher noch nichts sagen. So sei noch unklar, ob staatliche oder private Stellen die Drogen testen und ob die Untersuchungen in einem mobilen Labor – etwa auf Musikfestivals und vor Diskotheken – oder in einer stationären Einrichtung stattfinden sollen. Rechtlich umstritten ist, ob die Testenden während der Untersuchung die Drogen besitzen und sich somit strafbar machen. Weil sie die

Rauschmittel nicht selbst konsumieren wollen, gilt wohl auch nicht die Ausnahme für den Eigenbedarf. In den 90er Jahren ermittelte die Polizei gegen ein Berliner Drug-Checking-Projekt; die Staatsanwaltschaft erhob Anklage. Das Gerichtsverfahren wurde zwar nicht eröffnet, doch wurden die anonymen Drogentests eingestellt.

Heute gibt es in Deutschland keine derartigen Angebote. Die Geschäftsführerin vom Berliner Drogenhilfe-Verein Fixpunkt, Astrid Leicht, geht zwar davon aus, „dass das grundsätzlich erlaubt ist“. Doch traue sich keine Einrichtung, Drug-Checking anzubieten. „Das rechtliche Risiko besteht einfach. Deswegen fordern wir eine Klarstellung im Bundesgesetz.“ Nach ihrer Überzeugung gehe es ohne gesetzliche Änderungen, wenn sich die Akteure vor Ort einig seien. So könne es etwa in Berlin Absprachen geben, dass die Polizei nicht gegen die Tester ermittelt. An den Drogenkonsumenten sei die Polizei ohnehin wenig interessiert, sie konzentriere sich auf die Händler. Mobile Untersuchungslabors auf Großveranstaltungen seien sinnvoll. „Die sind zwar teurer, würden aber von mehr Menschen genutzt als stationäre Einrichtungen der Drogenhilfe.“

In Berlin ist die Regierung aus SPD und CDU der Meinung, dass die Drogentests nur mit einer Genehmigung des Bundesinstituts für Arzneimittel und Medizinprodukte zulässig seien, das dem FDP-geführten Gesundheitsministerium unterstellt ist. Momentan sei eine Erlaubnis unwahrscheinlich. Bei der Bundesbehörde selbst heißt es, die Frage lasse sich „nur im Zusammenhang mit einem konkreten Antrag beantworten“. In Niedersachsen kritisiert die neue schwarz-gelbe Opposition das Modellprojekt zum Drug-Checking, so die sozialpolitische Sprecherin der FDP-Fraktion, Sylvia Bruns: „Man kann die Drogen nicht verbieten und dann sagen: Der Staat zahlt dafür, dass die getestet werden.“ Auch die CDU warnt vor einer suggerierten „Scheinsicherheit“. Astrid Leicht vom Fixpunkt-Verein akzeptiert dieses Argument nicht. Bei den geplanten Drogentests werde natürlich darauf hingewiesen, „dass es immer riskant ist, Drogen zu nehmen“ (Werdermann, Sind meine Drogen clean www.taz.de 01.04.2013).

Nordrhein-Westfalen

Mordmotiv: Datenschutz

Ein 52jähriger Arbeitsloser ist am 05.04.2013 vom Landgericht Düsseldorf wegen heimtückischem Mord zu lebenslanger Haft verurteilt worden. Er hatte am 26.09.2012 Jahr seine Sachbearbeiterin im Jobcenter von Neuss, eine 32jährige Mutter erstochen, weil er ihr unterstellte, seine persönlichen Daten zu missbrauchen. Des Deutschen kaum mächtig, habe er Tage zuvor eine Datenschutzerklärung missverstanden und fälschlich mit illegalem Datenhandel in Zusammenhang gebracht, über den er einen Fernsehbeitrag gesehen hatte. Der Vorsitzende Richter Rainer Drees: „Der Angeklagte verstand weder genau was, noch warum er unterschreiben sollte.“ Er habe die Erklärung schließlich auf Drängen eines anderen Sachbearbeiters unterschrieben, die lediglich die Weitergabe der Daten an potenzielle Arbeitgeber regeln sollte. Am Tattag wollte er, so das Gericht, die Urheber des vermeintlichen Datenhandels „zur Verantwortung ziehen“. Vergeblich habe der Bruder des 2001 aus Marokko eingewanderten Landwirts versucht, ihn zu beruhigen und von der „fixen Idee“ des Datenmissbrauchs abzubringen.

Der Tat vorangegangen war, so der Vorsitzende, „ein Leben in zwei Welten“. 2001 kam der Täter nach Deutschland. Die Heirat mit einer Deutschen verschaffte dem Vater von 5 Kindern ein Bleiberecht. Er kam aus einem Dorf mit mittelalterlichen Strukturen und habe den Koran auswendig gelernt, bevor er mit 16 Jahren 3 Jahre lang eine staatliche Schule besuchte. Lese- und Schreibfähigkeiten waren „äußerst dürftig“. Er fand Jobs, unterbrochen von Phasen langer Arbeitslosigkeit. Dann zog er sich im 8. Stock eines Wohnhochhauses in Neuss in seine „andere Welt“ zurück. Eine Tötungsabsicht bestritt der Täter, er sei bei der Tat „nicht bei Verstand gewesen“. Die Anwälte von Eltern, Ehemann und Sohn des Opfers hatten als Nebenkläger ebenso wie die Staatsanwaltschaft die verhängte Höchststrafe beantragt. Dagegen hatten die Verteidiger die Tat nicht als Mord, sondern als Körperverletzung mit Todesfolge oder Totschlag gewertet. Sie kündigten Revision beim Bundesgerichtshof an (Kieler Nachrichten 06.04.2013, 11).

Sachsen

Spürhund sucht im Strafvollzug Mobiltelefone

Der sechsjährige belgische Schäferhund Artus Airport Lübeck soll nach Angaben des sächsischen Justizministers Jürgen Martens (FDP) die Vollzugsanstalten „im Kampf gegen unerlaubte Handykommunikation unterstützen“ und „den Verfolgungsdruck bei den Gefangenen deutlich steigern.“ Zuvor hatte der Hund an der Diensthundeschule das „Grundmodul Handyspürhund“ mit dem Prädikat befriedigend abgeschlossen. Nach Angaben des Ministers sind Mobiltelefone in den Gefängnissen des Freistaats „nicht ohne Grund nach Drogen die beliebteste Schmugglerware“. Allein in sächsischen Haftanstalten wurden im Jahr 2012 mehr als 300 Handys sichergestellt, obwohl die Geräte in deutschen Gefängnissen strikt verboten sind. Manche Vollzugsanstalten versuchen dem Problem mit Störsendern beizukommen, was kostspielig und problematisch ist. Der Empfang außerhalb der Justizvollzugsanstalten (JVA) darf durch die Handy-Blocker nicht erheblich gestört werden. Deshalb müssen viele verschiedene Sender mit geringer Leistung installiert werden. Dennoch gelingt diese Eingrenzung nicht immer. Zudem ist die teuere Technik zum Blockieren von UMTS-Signalen wenig nützlich, wenn das Handy eines Insassen über den neuen Standard LTE funkt. Mobiltelefone sind über die Jahre immer kleiner geworden und damit leichter zu verstecken. Mindestens zwei Stunden benötigen zwei Beamte, um eine Zelle gründlich zu durchsuchen. Artus soll es in fünf bis zehn Minuten schaffen. Seit November 2012 schnüffelt er zur Probe in seinem neuen Dienstsitz, der JVA Zeithain. Fünf Handys soll Artus dort bereits aufgetrieben haben.

Wie genau Artus Fährte aufnimmt, ist selbst seinem Diensthundeführer und den Ausbildern noch nicht klar. Vermutlich konzentriere er sich auf einen „Mischgeruch“ aus individuellen Anhaftungen am Gerät wie Schweiß, Haare und Schup-

pen sowie dem Eigenaroma elektrischer Geräte. Auf Erfahrungswerte können die Beamten bei der Klärung solcher Fragen nicht zurückgreifen. Es gibt Spürhunde, die auf Leichen, Schimmel oder sogar Krebsgeschwüre spezialisiert sind. Steffen Orthmann, Leiter Ausbildung und Prüfungswesen beim Bundesverband Wach- und Diensthunde (BVWD) meint: „Das ist mir ein bisschen suspekt, das ist schon sehr weit hergeholt.“ Allerdings überrascht es nicht, dass ausgerechnet Sachsen Pionierarbeit beim Apportieren leistet. Vor zwei Jahren war das Land das erste Mal mit seinem Tatendrang bei der Überwachung des Mobilfunks aufgefallen: Beim Gedenken an die Zerstörung Dresdens im Februar 1945 erhoben die Behörden über eine Funkzellenabfrage 138.000 Verbindungsdaten von Demonstranten und auch von Unbeteiligten (vgl. DANA 3/2011, 119ff.; Pollmer, Das Aroma am Handy, SZ 16./17.03.2013, 1; www.sueddeutsche.de 16.03.2013).

Schleswig-Holstein

Anonyme Spurensicherung für Vergewaltigungsopfer

Schleswig-Holstein wird wohl als erstes Bundesland eine flächendeckende anonyme Spurensicherung für vergewaltigte Frauen einführen. Eine entsprechende Initiative der Piratenpartei sowie einen Zusatzantrag der Regierungskoalition hat der Kieler Landtag an den Sozialausschuss überwiesen. Der Sprecher des Sozial- und Gesundheitsministeriums Frank Strutz-Pindor meinte: „Im Prinzip herrscht Einigkeit, dass das Anliegen völlig berechtigt ist. Die Frage ist, wie flächendeckend ein hohes Niveau erreicht werden kann.“

Die Initialzündung hatte eine Fachtagung des Landesverband Frauenberatung zum Thema „Streitsache Sexualdelikte – Frauen in der Gerechtigkeitslücke“ gegeben, wo den Parlamentariern vor Augen geführt wurde, dass Frauen, die Opfer sexualisierter Gewalt geworden sind, sehr oft erst ihren seelischen Ausnahmezustand verarbeiten und ihre Traumatisierung überwinden müssen, bevor es ihnen möglich ist, den Stress einer Anzeigenerstattung über sich ergehen zu lassen. Piratenabgeordneter Wolfgang Dudda erläuterte: „Die sofortige Anzeigenerstattung verlangt das erneute Durchleben der Tat gegenüber einer fremden Person, ohne die Tat seelisch verarbeitet zu haben“. So sei auch zu erklären, dass nur ein Bruchteil der Fälle sexualisierter Gewalt gegen Frauen über 16 Jahren zur Anzeige komme. Für eine spätere Verurteilung des Vergewaltigers seien Frauen oft auf die ihre Aussage stützenden Spuren angewiesen, wenn nicht später vor Gericht die Situation „Aussage gegen Aussage“ eintreten solle oder sie mit entwürdigenden „Vergewaltigungsmythen“ wie Rache-Motiven konfrontiert werden möchten. Diese Spurensicherung muss i. d. R. binnen 24 Stunden nach der Vergewaltigung erfolgen.

Diese „Gerechtigkeitslücke“ soll dadurch geschlossen werden, dass die Klinken im ganzen Land in die Lage versetzt werden, Spuren einer Vergewaltigung wie DNA-Absonderungen, Sperma-Rückstände und Faserpartikel anonymisiert sicherzustellen. In den Städten Hamburg, Bremen und Hannover gibt es schon derartige Angebote. Die Spurensicherungssets kosten nach Auskunft der Polizei rund acht Euro. Der Gebrauch sei, so Dudda, durch die Polizei leicht vermittelbar. „Es müsste also nur eine Vereinbarung des Sozialministeriums mit den Krankenhäusern zur Kostenübernahme abgeschlossen werden.“

Eine Vergewaltigung bedeutet für jeder Frau eine massive Verletzung ihrer körperlichen Unversehrtheit im sensiblen Bereich ihrer sexuellen Selbstbestimmung. In besonders schweren Fällen, wenn eine Vergewaltigung mit dem Einsatz einer Waffe durchgesetzt wird, sieht das Gesetz eine Haftstrafe von bis zu zehn Jahren vor. 326 Vergewaltigungen sind in Schleswig-Holstein im Jahr 2012 laut Innenministerium angezeigt worden. Bundesweit waren es um die 12.000 Taten. Die Dunkelziffer liegt schätzungsweise 20-mal höher.

Der Leiter des Instituts für Rechtsmedizin am Universitätsklinikum Schleswig Holstein (UKSH) Professor Hans-Jürgen Kaatsch sicherte zu, mit seinem Team Schulungen der Ärzte an den Krankenhäuser vornehmen zu können. Die Lagerung der sichergestellten Körperspuren könnten mit einem chiffrierten Code fachgerecht an den beiden UKSH-Standorten in Lübeck und Kiel erfolgen. „Die Hoheit über die Chiffre soll jedoch das Opfer haben“, so Dudda. „Die Möglichkeit der anonymen Spurensicherung schließt also die Gerechtigkeitslücke. Wie viel leichter könnte ein Vergewaltigungsopfer in ein Strafverfahren gehen, wenn es weiß, dass seine Tatdarstellung durch gesicherte Spuren untermauert sind.“

Die anonyme Spurensicherung und -lagerung erleichtert es auch Frauen, Vergewaltiger, die aus dem persönlichen Umfeld stammen – was immerhin in mehr 66% der Täter der Fall ist –, erst später anzuzeigen und vor Gericht zu bringen. Dudda: „Dann ist genügend Zeit gewesen, den sozialen Rückzug zu organisieren, so dass nicht auf einen Schlag das gesamte soziale Gefüge einstürzt.“ Auch Ministeriumsprecher Strutz-Pindor hält eine „lebensnahe Lösung“ für unverzichtbar. „Über die gesicherten Spuren muss allein das Opfer entscheiden, was damit geschieht“ (von Appen, Spurensicherung ohne Brimborium, www.taz.de 01.04.2013).

Datenschutznachrichten aus dem Ausland

Europa

„Smart Borders“ - elektronische Grenzüberwachung

Die Kommission der Europäischen Union (EU) hat ihre Pläne für ein Ein- und Ausreisesystem nach US-Vorbild und ein Vorzugsprogramm für Vielreisende konkretisiert. Am 28.02.2013 stellte Innenkommissarin Cecilia Malmström in Brüssel einen Verordnungsentwurf „Smart Borders“ vor, wonach AusländerInnen sich künftig mit allen zehn Fingerabdrücken bei der Einreise in die EU von der Grenzkontrolle registrieren lassen müssen. Außerdem sollen Zeitpunkt und Ort der Einreise und Ausreise von Drittstaatsangehörigen erfasst werden. Die Kosten für das Paket sind mit 1,1 Mrd. Euro veranschlagt. Der Entwurf würde nach der Verabschiedung durch das EU-Parlament und den EU-Rat direkt in allen Mitgliedsstaaten rechtsgültig (COM(2013)95, 97 final, BR-Drs. 180/13).

Das neue elektronische System soll die zulässige Dauer eines Kurzaufenthalts automatisch berechnen und einen Warnhinweis an die nationalen Sicherheitsbehörden erzeugen, wenn die oder der Betreffende bis zum Ablauf der Aufenthaltsdauer nicht ausgereist ist, insbesondere bei Kurzzeitvisa. Die Mitgliedsstaaten stützen sich bislang bei der Kontrolle von Angehörigen aus Drittstaaten vor allem auf die in einem Reisedokument eingetragenen Stempel; das erscheint der Kommission zu zeitraubend und unzuverlässig. Zudem könne der „ständig wachsende Strom von Reisenden in die und aus der EU“ ohne Nutzung neuester Technik nicht bewältigt werden. Pate gestanden haben die US-Systeme Esta für elektronische Reisebewilligungen und Visit zur biometrischen Erfassung Einreisender.

Zweiter Teil des Pakets „Intelligente Grenzen“ ist ein Vorzugsprogramm. Dabei sollen automatische, biometriegestützte Schleusen etwa an Flughäfen eingesetzt werden, die auch auf Gesichtserkennung mit 3D-Technik und elektronische Reisepässe setzen. Die Privilegierung setzt den Einsatz einer 20 Euro teuren Chipkarte voraus. Die Kommission hofft, dass registrierte TeilnehmerInnen, die zum Beispiel ihre Fingerabdrücke abgegeben haben, so „sehr viel schneller abgefertigt werden können“. Ideal sei das Programm etwa für Geschäftsreisende, Zeitarbeitskräfte, WissenschaftlerInnen und Studierenden sowie Drittstaatsangehörige mit enger Verwandtschaftsbeziehung zu EU-BürgerInnen, die eine Grenze zur EU mehrmals im Jahr übertreten. Die Daten sollen in der Regel sechs Monate lang gespeichert bleiben.

Die Grünen im EU-Parlament sehen mit dem Entwurf, dessen Komponenten 2017 oder 2018 in Betrieb gehen können, „alle Grenzen gesprengt“. Die grenzpolitische Sprecherin der Fraktion, Ska Keller, meint, der Entwurf sei der Einstieg in Big Brother und die Kompletterfassung von Reisenden in die EU. „Unerwünschte Drittstaatenangehörige“ könnten bereits jetzt identifiziert und abgewiesen werden, sodass eine neue „Datenkrake“ nicht erforderlich sei. Auch sehe die Kommission schon jetzt eine Zweckentfremdung der Fingerabdruckdaten vor: Die Polizeibehörden sollen auf die Datenbank zumindest theoretisch zugreifen können. AusländerInnen würden „in eine Ecke mit Verbrechern“ gestellt.

Kellers innenpolitischer Kollege Jan Philipp Albrecht rügte, dass die Kommission viel Geld verprassen wolle, „das bei Polizei und Justiz vor Ort und der Zusammenarbeit via Europol und Eurojust schon heute fehlt“. Vielreisende würden zudem nach ihrer vermeintlich „freiwilligen Registrierung“ verdachtsunabhängig überwacht und diskriminiert. Dabei habe Brüssel bislang nicht belegt, dass die geplanten „Massendatenspeicherungen“ mehr Sicherheit brächten.

Der Bundesdatenschutzbeauftragte Peter Schaar hält die Pläne für vollautomatisierte Kontrollen an den EU-Außengrenzen für nicht praktikabel und rechtlich untragbar. Das Smart-Border-System verletze Grundrechte. Wegen technischer Defizite könnten unbescholtene Reisende in Fahndungslisten auftauchen und dann wie Kriminelle behandelt werden. Das Konzept sei völlig unrealistisch und Geldverschwendung: „Die Pläne sind alles andere als smart.“ Laut Schaar sollte in den USA vor einigen Jahren ein ähnliches System eingeführt werden. Das funktioniere bis heute nicht, obwohl der Grenzfluss in die USA mit nur zwei direkten Nachbarstaaten viel einfacher zu koordinieren sei als die Ein- und Ausreisen in der EU. Hinzu komme, dass das Vorhaben als „lückenlose Vorratsdatenspeicherung“ juristisch nicht haltbar sei. Er hoffe, dass sich die Bundesregierung bei den anstehenden Beratungen und Verhandlungen in Brüssel „sehr kritisch“ positioniere. Auch die EU-Datenschutzbeauftragten haben das Programm als unverhältnismäßig kritisiert.

Verschiedene Studien kommen ebenfalls zu vernichtenden Ergebnissen. Die Autoren einer von der Böll-Stiftung in Auftrag gegebenen Studie namens „Borderline“ meinen, die enormen Kosten stünden in keinem Verhältnis zum Nutzen. Die Aussage, das Programm könne das Leben von Bootsflüchtlingen retten, die immer wieder im Mittelmeer ertrinken, hält Mitautor Ben Hayes für vorgeschoben. Von Rettung der Flüchtlinge stehe in den Konzepten nichts, vielmehr würden „Push-Back“-Pläne entwickelt, die dazu dienten, Menschen abzuschrecken oder noch auf dem Meer zurückzuschicken. Ebenso wie der zusätzlich geplante Überwachungsapparat Eurosur würden die Menschenrechte nicht ausreichend beachtet; ein effizientes Funktionieren sei nicht zu erwarten. Auch eine von der EU selbst in Auftrag gegebene Studie bezweifelt den Nutzen des Programms. Datenschutz und das Recht auf Privatsphäre könnten dadurch verletzt werden, so die Autoren (Krempl, Smart Borders: EU-Kommission beschließt elektronische Grenzüberwachung, www.heise.de 28.02.2013; Mit Chipkarte in die EU, SZ 01.03.2013;

Biermann, EU-Pläne zur Grenzüberwachung „verletzen Grundrechte“, www.zeit.de 05.03.2013).

Frankreich

Polizei kontrolliert verdeckt Geschwindigkeit

Die französische Polizei ist künftig auf den Straßen des Landes mit Zivilfahrzeugen unterwegs, die ein Radarsystem im Nummernschild versteckt haben.

300 Zivilfahrzeuge sollen in den kommenden Jahren rasende Autos überführen und für mehr Sicherheit auf französischen Straßen sorgen. Auf Autobahnen in Frankreich gilt ein allgemeines Tempolimit von 130 km/h. Die meisten VerkehrsteilnehmerInnen halten sich daran, denn Rasen ist teuer. Wer 20 km/h zu schnell unterwegs ist, muss mindestens 135 Euro zahlen, wer mehr als 50 km/h zu schnell ist, dem droht ein Bußgeld von 1.500 Euro.

Die Zivilfahrzeuge sind mit unsichtbarem Infrarot-Blitz in der vorderen Stoßstange ausgestattet. Eine Radarantenne liegt hinter dem Nummernschild versteckt, eine Kamera befindet sich auf dem Armaturenbrett, daneben ein Bildschirm mit Touchscreen. Die Rechenzentrale mit eigener Batterieversorgung ist im Kofferraum untergebracht. Gemessen wird unauffällig, beispielsweise während eines Überholmanövers. Dabei kann das polizeiliche Zivilfahrzeug die vorgegebene Geschwindigkeitsbeschränkung einhalten. Überholt ein Fahrzeug mit einem Tempo, das mindestens 20 Stundenkilometer über dem erlaubten Limit liegt, beginnt die Messung. 10% Toleranz wegen möglicher Messfehler werden abgezogen. Wem dann noch ein Tempoverstoß nachgewiesen wird, die oder der bekommt erst Wochen später Post mit einer Zahlungsaufforderung. VerkehrssünderInnen sollen nicht sofort an Ort und Stelle angehalten werden.

Ab 2014 soll die Technik weiter verbessert werden. Dann können auch Messungen aus der Gegenrichtung erfolgen. Die neue Radartechnik soll überwiegend in dem aktuellen Renault Mégane dCi eingebaut werden, einem Auto, das in Frankreich so häufig ist wie in Deutschland der VW Golf. Ausgerüstet mit der kompletten Messtechnik wird der Wagen insgesamt 70.000 Euro kosten. Pro Jahr sollen 100 solcher Fahrzeuge angeschafft werden. Auch in Motorräder soll die Technik eingebaut werden.

Zur Sicherheit auf französischen Straßen sollte auch die neue Vorschrift beitragen, dass grundsätzlich alle AutofahrerInnen in Frankreich einen Alkoholtest im Auto bei sich haben müssen. Das Gesetz, das im vergangenen Jahr noch von der Sarkozy-Regierung erlassen wurde, war von Beginn an umstritten. Wegen Lieferschwierigkeiten und vor allem Ungenauigkeiten der Geräte hagelte es Kritik. Aus diesem Grund hat die neue französische Regierung nicht einmal ein Jahr später die neue Vorschrift wieder gekippt. Frankreichs Innenminister Manuel Valls versicherte, für ihn gebe es „keine verpflichtenden Alkoholtests und erst recht keine Sanktionen“ für FahrerInnen, die kein Pusteröhrchen in ihrem Auto haben. Alkoholkonsum ist in Frankreich für rund ein Drittel der Toten auf den Straßen verantwortlich (Kubisch, Französische Polizei blitzt mit dem Kennzeichen, www.welt.de 19.03.2013).

Großbritannien

Scotland Yard nutzte Identitäten toter Kinder

In Großbritannien sorgen die Ermittlungsmethoden einer Spezialeinheit von Scotland Yard für Aufregung; ein Untersuchungsausschuss soll Aufklärung bringen: Verdeckte Ermittler nutzten zwischen 1968 und 1994 die Identitäten von rund 80 verstorbenen Kindern, gaukelten Frauen Beziehungen vor und verschwanden wenig später spurlos. Ein Beispiel: Zwei Jahre lang war ein Frau mit John Barker zusammen. Im März 1992 verschwand er plötzlich aus ihrem Leben. Die Frau suchte nach einer Erklärung dafür, heuerte einen Privatdetektiv an und verfolgte Spuren 18 Jahre lang in aller Welt. Heute weiß sie, dass ihr Ex-Freund ein verdeckter Ermittler von Scotland Yard war, der für seine Tarn-Identität den Namen eines verstorbenen Jungen genutzt hat. Der echte John Barker war 1968 im Alter von acht Jahren an Leukämie gestorben. Die Eltern wussten, wie in allen Fällen, nichts davon. Drei Jahrzehnte lang hatte die Metropolitan Police (MET) Geburts- und Sterberegister als Quellen genutzt.

In der Presse schilderten zwei Ermittler, die anonym bleiben, detailliert, wie sie und weitere Kollegen sich der Identitäten bedienten, teilweise mit Gewissensbissen. Einer der Beamten sagte, er habe sich gefühlt, als „trampele er auf dem Grab“ des Vierjährigen herum, dessen Namen er angenommen hatte, um in den neunziger Jahren in einer Anti-Rassismus-Gruppe verdeckt zu ermitteln. Die beiden Polizisten arbeiteten gemäß dem Bericht für die Special Demonstration Squad (SDS). Die geheime Abteilung von Scotland Yard war 1968 gegründet worden, nachdem vor der US-Botschaft in London eine Demonstration gegen den Vietnamkrieg eskaliert war. Ermittler sollten Protestbewegungen von innen überwachen und wurden, als Tierschützer oder Friedensaktivisten getarnt, in die entsprechenden Organisationen eingeschleust. Jahrelang sammelten sie dort Informationen. 2008 wurde die SDS laut Presseberichten aufgelöst.

Die MET betont, dass diese Praxis heute nicht erlaubt sei. Zu den früheren Absprachen für Undercover-Identitäten von SDS-Polizisten würden Ermittlungen eingeleitet. Etwa seit 2011 kocht das Thema um die britischen Spezialermittler immer wieder hoch. Damals kam der Fall von Mark Kennedy ans Tageslicht, der von 2002 bis 2009 im Auftrag von Scotland Yard undercover in der militanten Umweltaktivistenszene aktiv war, zunächst in Großbritannien, danach in ganz Europa. Nach Angaben von Mitstreitern hatte er als Agent provocateur viele Proteste angeheizt. Außerdem hatte er mit mehreren Frauen Affären; mit einer war er sechs Jahre zusammen. Inzwischen befasst sich ein parlamentarischer Untersuchungsausschuss mit den Fällen. Elf Frauen haben die MET verklagt, weil sie „sehr persönliche“ Beziehungen zu Agenten hatten, ohne deren wahre Identität zu kennen. Die Ermittler lebten mit den Frauen, einige bekamen gar gemeinsame Kinder. Nach Abschluss ihres Auftrags verschwanden sie einfach spurlos. Ein Uno-Vertreter hat sich inzwischen

eingeschaltet. Maina Kiai forderte Ende Januar 2013 bei einem zehntägigen Recherchebesuch in London, Belfast und Edinburgh eine öffentliche Aufarbeitung des Falls Kennedy und ähnlicher Fälle: „Es ist inakzeptabel, dass ein Staat jemanden bezahlt, der Frauen ausnutzt, Teil ihres Lebens wird und sie dann einfach verlässt und vernichtet. Das ist kein James-Bond-Film.“ Das Vorgehen verletzte die Menschenrechte und das Recht auf Privatsphäre; die ausspionierten Gruppen seien nicht in kriminelle Machenschaften verwickelt gewesen.

Das Innenministerium erklärte, erste interne Ermittlungen seien bereits durchgeführt und Vorschläge für den Einsatz von Langzeitermittlern wie Kennedy vorgelegt worden: „Die Regierung arbeitet mit der Polizei an der Umsetzung dieser Empfehlungen.“ Schon im März 2010 schilderte ein Pressbericht ausführlich, wie Dutzende Undercover-Ermittler ihre Legenden auf der Identität von Toten aufbauten. Die Methode, die Frederick Forsyth in seinem Thriller „Der Schakal“ beschreibt, sei vor rund 40 Jahren eingeführt worden, um Ermittlern eine glaubhafte Biografie zu bieten. Die Fahnder besuchten beispielsweise das Geburtshaus ihres Namensgebers, sahen sich die Umgebung an und speicherten kleine Details ab, um ihre Tarnung möglichst echt erscheinen lassen zu können. Gemäß Presseberichten wurde diese Form der Legendenbildung Mitte der neunziger Jahre mit der Digitalisierung von Daten und der Popularisierung des Internet eingestellt. Allerdings soll es einen Fall geben, in dem ein Ermittler noch 2003 die Identität eines toten Kindes genutzt hat.

Ein parlamentarischer Untersuchungsausschuss wird sich künftig mit dem zweifelhaften Vorgehen befassen. Der Ausschussvorsitzende Keith Vaz erklärte: „Der Ausschuss wird nun von der Polizei Erklärungen verlangen müssen, wie es zu diesen grausamen Methoden kommen konnte. Das bedeutet enormes Leid für die Familien, die erfahren, was mit der Identität ihrer verstorbenen Kinder geschehen ist“ (Utler, Scotland Yard: Undercover-Ermittler benutzten Namen toter Kinder, www.spiegel.de 04.02.2013).

Österreich

Neue Datenschutzbehörde übernimmt Aufgaben der Datenschutzkommission

Der Verfassungsausschuss des österreichischen Nationalrats hat auf das Urteil des Europäischen Gerichtshofes vom 16.10.2012 reagiert, wonach die bisherige Datenschutzkommission nicht unabhängig genug ist, und die Novelle des Datenschutzgesetzes beschlossen, welche die Einrichtung einer neuen Datenschutzbehörde vorsieht. Diese wird nicht nur als unabhängige Kontrollstelle zur Überprüfung der Einhaltung von Datenschutzvorschriften fungieren, sondern unter anderem auch für die Führung von Registrierungsverfahren, die Genehmigung von Datenübermittlungen ins Ausland, die Genehmigung von Datenverwendungen für wissenschaftliche oder statistische Zwecke und die Auskunftserteilung an Bürger zuständig sein. Der Leiter bzw. die Leiterin der Datenschutzbehörde soll für jeweils fünf Jahre vom Bundespräsidenten auf Vorschlag der Regierung bestellt werden.

Bescheide der neuen Datenschutzbehörde können beim Bundesverwaltungsgericht angefochten werden, wobei die Entscheidungen dort ein Senat unter Einbindung fachkundiger Laienrichter aus dem Kreis der Arbeitgeber und der Arbeitnehmer treffen wird. Ein jährlich zu erstellender Bericht der Datenschutzbehörde soll auch dem Nationalrat und dem Bundesrat übermittelt werden.

Von der ursprünglich vorgesehenen Einrichtung eines Fachbeirats zur Unterstützung der Datenschutzbehörde wurde letztendlich abgesehen. Man wolle jeglichen Zweifel an der Unabhängigkeit der Datenschutzbehörde vermeiden, hieß es dazu in den Erläuterungen zu einem am 19.04.2013 gemeinsam von SPÖ, ÖVP und FPÖ vorgelegten Abänderungsantrag. Außerdem wurde durch eine Umformulierung des Gesetzentwurfs deutlicher sichtbar gemacht, dass nicht nur öffentliche Auftraggeber in Verfahren vor der Datenschutzbehörde Parteistellung erhalten. Der Datenschutzrat erhält die ausdrückliche Erlaubnis, Gutachten zu Fragen von grundsätzlicher Bedeutung des Datenschutzes einzuholen (Verfassungsausschuss billigt Novellierung des Datenschutzgesetzes, www.ots.at 19.04.2013).

Schweiz

Nestlé und Securitas zahlen an Spitzelopfer

Vom Nestlé-Konzern wurde ein Urteil des Zivilgerichts von Lausanne akzeptiert, welches das Unternehmen wegen der Verletzung von Persönlichkeitsrechten für schuldig erklärt hat. Hintergrund ist eine Bespitzelung und Infiltration einer Attac-Gruppe in Lausanne, die den Konzern öffentlich kritisiert hatte. Die Gruppe wurde im Auftrag von Nestlé durch die Sicherheitsfirma Securitas ausgehorcht. Eine Securitas-Mitarbeiterin gehörte zeitweise zur Attac-Gruppe und arbeitete an einem Buch über Nestlé mit. Zugleich stellte sie für den Konzern Dossiers über die Mitglieder der Gruppe zusammen. Später wurde sie enttarnt. Nestlé und Securitas wurden verurteilt, jedem der acht Geschädigten 3.000 Schweizer Franken an „moralischer Wiedergutachung“ zu zahlen. Beide Firmen akzeptierten das Urteil Mitte März 2013 (Der Spiegel 13/2013, 68).

Rußland

FSB kontrolliert soziales Netzwerk VKontakte

Eine russische Zeitung hat aufgedeckt, dass das soziale Netzwerk „VKontakte“ offenbar Daten von Kreml-GegnerInnen an den Inlandsgeheimdienst FSB weiterleitet. VKontakte wurde 2006 gegründet und zählt 200 Millionen Mitglieder; es ist die wichtigste Austausch- und Werbeplattform des Landes. Facebook hat in Russland dagegen nur knapp 7 Millionen Nutzende. Pawel Durow, der Gründer von VK, besitzt ein Vermögen von 200 Millionen Euro, eine Million hat er an

Wikipedia gespendet. Er ist 28 Jahre alt und wird mit Mark Zuckerberg verglichen. Im Dezember 2011, als Zehntausende RussInnen gegen die Ergebnisse der Parlamentswahl demonstrierten, setzte der Kreml Durow unter Druck. VK-Profile von Oppositionellen sollten entfernt werden. Durow postete damals das schriftliche Ersuchen trotzig in seinem eigenen Profil; daneben das Bild eines Hundes mit ausgestreckter Zunge: „Meine offizielle Antwort an die Geheimdienste."

Gleichzeitig soll er aber laut dem Pressebericht einen Brief an Wladislaw Surkow geschrieben haben, ehemals Chefideologe im Kreml: „Wie Sie wissen, arbeiten wir seit Jahren mit dem FSB und der Abteilung K des Innenministeriums zusammen, indem wir die Informationen von Tausenden unserer Nutzer in Gestalt von IP-Adressen und Handynummern reibungslos weiterleiten. Wir sind besorgt über die Perspektive einer Destabilisierung im politischen und wirtschaftlichen Leben Russlands und sind bereit, weiterhin an der Seite der Behörden alles zu unternehmen, um eine Verbreitung von Gewalt und Chaos zu verhindern." Profile von Oppositionellen zu entfernen, sei aber nicht im Interesse Russlands. Dann würden nämlich viele junge NutzerInnen zu Facebook wechseln. „Langfristig könnte das unsere technologischen und ideologischen Bemühungen, den Andrang ausländischer Sozialnetzwerke auf dem Heimatmarkt zu bremsen, zunichtemachen." Außerdem würden die Unzufriedenen dann ihre Protestmärsche auf Facebook planen - unbeaufsichtigt.

Entweder solle, so Durow, der Kreml seine diskrete Kontrolle im Netz fortsetzen, oder man führe eine totale Zensur nach chinesischem Vorbild ein, die auch Facebook träfe - aber bitte keine Mittelwege. In einem anderen dem Presseorgan vorliegenden Schreiben schildert ein ehemaliger VK-Pressesprecher, wie er fiktive Profile von Oppositionsgruppen anlegte, um Verwirrung zu stiften. Durow ließ den Zeitungsbericht als „völligen Blödsinn" dementieren. Viele VK-Nutzende haben trotzdem ihren Austritt angekündigt (Neshitov, Geheimdienst liest mit, SZ 28./29.03.2013, 1).

USA

Inhaltsaufzeichnung von digitaler Kommunikation

Tim Clemente, ehemaliger Anti-Terror-Agent des FBI, ehemaliger Polizist und ehemaliger Armeeangehöriger, bestätigte in zwei CNN-Fernsehauftritten, dass Sicherheitsdienste der USA jede Form digitaler Kommunikation innerhalb des Landes aufzeichnen und dass diese auch im Ausland aktiv sind. Im Zusammenhang mit dem Bombenattentat auf den Marathon in Boston führte er aus, dass das FBI auch zurückliegende Telefonate abrufen kann: „Natürlich haben wir bei Untersuchungen zur Nationalen Sicherheit Wege herauszufinden, was exakt in diesen Gesprächen gesagt wurde." Damit bezog er sich auf Telefongespräche zwischen dem inzwischen verstorbenen Attentäter und dessen Frau. Die Inhalte dieser Unterhaltungen stünden dem FBI auch dann zur Verfügung, wenn die Frau sie nicht von sich aus preisgeben sollte. „Das ist nicht unbedingt etwas, was das FBI vor Gericht präsentieren würde, aber es könnte die Untersuchung voranbringen oder zu einem Verhör der Frau führen. Wir können das natürlich herausfinden."

Auf die ungläubige Rückfrage der CNN-Fernsehjournalistin sagte Clemente: „Willkommen in Amerika. Alles was wir sagen, wird erfasst, während wir sprechen, ob uns das gefällt oder nicht." Tags darauf bestätigte er seine Aussagen: „Im Bereich der Nationalen Sicherheit, der Bundesregierung, haben wir Möglichkeiten, viele Möglichkeiten, zu unserer Verfügung, quer durch die verschiedenen Geheimdienste. Nicht nur im Inland, sondern auch in Übersee. Diese Möglichkeiten erlauben uns, Information zu erlangen, die wir normalerweise nicht in einer strafrechtlichen Untersuchung verwenden können, die aber für große Terroruntersuchungen oder zur Spionageabwehr genutzt werden." Auf die Frage „Sie sprechen nicht über Nachrichten auf einem Anrufbeantworter. Worüber sprechen Sie genau?" erwiderte Clemente: „Ich spreche über jegliche digitale Kommunikation. Es gibt einen Weg, digitale Kommunikation aus der Vergangenheit anzuschauen." Er könne jedoch keine Details dazu nennen, wie das genau gemacht werde. „Aber ich kann Ihnen sagen, dass keine digitale Kommunikation sicher ist." Die Ermittler würden die Inhalte der Telefongespräche zwischen dem Attentäter und seiner Frau eruieren.

Völlig neu sind diese Hinweise auf den Umfang der Überwachung nicht. Die britische Zeitung Guardian listet in einem Artikel mehrere Fälle auf, in denen ähnliche Informationen von Eingeweihten bekannt wurden, etwa von einem Mitarbeiter des Telekommunikations-Anbieters AT&T, Mark Klein, oder von William Binney. ehemaliger Mitarbeiter des US-Geheimdiensts NSA (National Security Agency). In einem Interview mit Democracy Now im April 2012 sagte Binney, die NSA zeichne fast alle E-Mails auf. Seiner Schätzung nach, die auf Angaben aus 2006 fuße, habe die NSA eine Größenordnung von 20 Billionen Unterhaltungen in Form von E-Mails und Telefonaten zwischen US-Bürgern erfasst. Finanzielle Transaktionen seien in dieser Zahl noch nicht enthalten. Bei einer parlamentarischen Anhörung stellt dagegen ein NSA-General in Abrede, dass Kommunikation zwischen US-Bürgern routinemäßig „abgefangen" werde (intercepted). 2015 wollen NSA und DISA (Defense Information Systems Agency) ein neues Datencenter in Betrieb nehmen. Der Bauauftrag im Wert von 565 Millionen US-Dollar wurde im März 2013 vergeben (Sokolov, Ex-Terrorfahnder: Keine digitale Kommunikation ist sicher, www.heise.de 05.05.2013; Greenwald, Are all telephone calls recorded and accessible to the US government? www.guardian.co.uk 04.05.2013).

USA

Banken-Polizei-Kooperation bei Videokontrolle in New York

Wie das Magazin CounterPunch im Gefolge der Sendung „60 Minutes" herausfand, befindet sich unter der Adresse 55 Broadway in New York ein polizeiliches Überwachungszentrum für die Stadt unter dem Namen Lower Manhattan Security Coordination Center. Am Eingang des Gebäudes stehen weitere

prominente Namen: Goldman Sachs, Citigroup, JPMorgan Chase ... Die Lower Manhattan Security Initiative wurde für 150 Millionen Dollar aus Steuergeldern finanziert. Die Kosten, Tendenz steigernd, werden von der Regierung in Washington und der Stadt New York getragen. Die Terminals sind rund um die Uhr besetzt. Etwa 2.000 private Überwachungskameras gehören den Firmen der Wall Street, 1.000 sind im Eigentum der New Yorker Polizei. Zusätzliche 700 Kameras sind in Midtown installiert und liefern ihre Bilder in das Zentrum. Die technische Ausrüstung ist so perfekt, dass praktisch jede Bewegung jedes Menschen auf Computern in Real-Time ausgewertet, vergrößert, scharf gestellt werden kann. Eine Sprecherin des Überwachungs-Zentrums sagte in der Sendung „60 Minutes", sie könne „mit einem Fingerschnippen" jede Aktion der ahnungslosen Bürger isolieren und dokumentieren.

Der Bürgermeister von New York Michael Bloomberg ist Initiator des Zentrums. Polizeichef Raymond Kelly ist auf die gute Zusammenarbeit der Banken mit der Polizei stolz. Deren Rechtmäßigkeit ist umstritten. Für die Überwachungsaktion gibt es kein Gesetz, keine Kontrolle und keine öffentlich einsehbaren Dokumente. Der New York Code verbietet in seiner Section 700.15 ausdrücklich die Videoüberwachung ohne richterliche Anordnung. Die New York Civil Liberties Union (NYCLU) wies auf diesen Umstand mehrfach hin. Bloomberg erklärte die flächendeckende Überwachung dagegen als unvermeidlich. Die Weiterentwicklung der Technologie sei nicht mehr aufzuhalten: „Gewöhnen Sie sich an Big Brother!". In seiner wöchentlichen Radio-Ansprache am 22.03.2013 meinte er: „Jeder möchte natürlich seine Freiheit behalten, aber ich weiß nicht, wie man das erreichen kann." Es sei „verrückt", gegen die Überwachungstechnologie zu argumentieren. In fünf Jahren werde es überall Kameras geben: „Wo ist der Unterschied, ob die Drohne in der Luft schwebt oder am Gebäude installiert ist? Wir sind auf dem Weg in eine andere Welt." In dieser gebe es mehr Sichtbarkeit und weniger Privatsphäre. „Ich weiß nicht, wie man das aufhalten kann."

Seit dem 11. September 2001 ist man in New York verstärkt vorsichtig geworden. Die Initiative „Ring of Steel" vernetzt die Überwachungskameras von Polizei, Banken und anderen Institutionen auf den öffentlichen Plätzen in Manhattan. Die enge Zusammenarbeit der Polizei mit den Wall Street Banken in New York ist erst kürzlich bekanntgeworden. Die Erfahrungen der Bewegung „Occupy Wall Street" (OWS) hatten dazu geführt, dass die Banken die Polizei konkret beraten, wie sie bei der Überwachung vorgehen soll (New York: Wall Street und Polizei betreiben gemeinsam Video-Überwachung, Drohnen über New York: „Gewöhnen Sie sich an Big Brother!", deutsche-wirtschafts-nachrichten.de 27.03.2013.

USA

Hacker veröffentlichen sensible Daten von Prominenten

Unbekannte veröffentlichten über die Adresse „exposed.su" persönliche Informationen von US-Stars und Politikern, darunter Jay-Z, Beyoncé, Mel Gibson, Ashton Kutcher, Arnold Schwarzenegger, Vize-Präsident Joe Biden, Hillary Clinton, Sarah Palin, Al Gore, Justizminister Eric Holder, FBI-Chef Robert Mueller, Bill Gates, Tom Cruise, Tiger Woods, der letzte US-Präsidentschaftskandidat der Republikaner Mitt Romney, TV-Sternchen Kim Kardashian, Paris Hilton, Britney Spears, der Immobilien-Mogul Donald Trump und Michelle Obama. Auf Englisch stand „Geheimakten" über der dunklen, mit gespenstischer Musik und schwarzem Hintergrund unterlegten Webseite. Millionen BesucherInnen haben die anonyme Internetadresse, die unter dem Namenskürzel der ehemaligen Sowjetunion registriert ist, angeklickt. Was sie dort zu lesen bekamen, beschäftigt die Polizei in Los Angeles, das FBI, den US-Geheimdienst und das Weiße Haus. Veröffentlicht wurden Kontaktdaten wie Telefonnummern und Adressen, Sozialversicherungsnummern, Kontostände, Kredithistorie und Hypothekenzahlungen ihrer prominenten Opfer. Die Sozialversicherungsnummer ist ein wichtiges Identifizierungsmerkmal in den USA für Vertragsabschlüsse.

Präsident Obama erklärte zu dem neuem Angriff in einem Interview: „Wir sollten nicht überrascht sein, dass sich Hacker Zugang zu privaten Informationen verschaffen können. Wir stehen hier vor einem wirklich großen Problem." Die veröffentlichten Daten der First Lady kommentierten die Hacker mit den Sätzen: „Du kannst dich bei deinem Ehemann bedanken. Dich lieben wir weiterhin, Michelle." Secret-Service-Sprecher Brian Leary bestätigte, dass man „Ermittlungen aufgenommen" habe. Ob die Cyber-Piraten die richtigen Daten ihrer prominenten Opfer veröffentlicht haben, war zunächst unklar. FBI-Agent Brad Garrett machte sich zur Motivation der Täter Gedanken: „Das macht für mich eigentlich keinen Sinn." Computerhacker würden sich in die Konten ihrer Opfer einklicken, um Geld zu stehlen. Bisher sei das aber nicht passiert. „Ich würde mich nicht wundern, wenn alles nur ein böser Witz ist." Die Telefonnummern der First Lady waren alt und mittlerweile inaktiv, eine Verbindung ins Weiße Haus bekommt man mit ihnen nicht. Unklar ist, ob der Multi-Millionär Jay-Z tatsächlich 227.000 Dollar Kreditkartenschulden hat, wie die Hacker mit ihren veröffentlichten Daten behaupteten. Wie Jay-Z haben die meisten betroffenen Stars zu den Cyber-Angriffen bisher nicht bestätigt, ob ihre veröffentlichten Informationen korrekt sind. Der Polizeichef von Los Angeles, Charles Beck, erklärte dagegen, dass seine Daten richtig sind. Beck scheint damit schon Erfahrungen zu haben. Polizeisprecherin Sara Faden: „Das kommt immer mal wieder vor" (Remke, Hacker veröffentlichen Nummer von Michelle Obama, www.welt.de 13.03.2013, Bill Gates Bankkonten von Hacker bloßgestellt, www.t-online.de 13.03.2013; Hacker veröffentlichen hochsensible Promi-Daten, www.focus.de 13.03.2013; Hacker veröffentlichen „Geheimakten" von Stars, SZ 13.03.2013, 10).

USA/weltweit

Nach Datendiebstahl größter Online-Bankraub

Cyber-Räubern gelang es, in zehn Stunden in 26 Ländern Bargeld 40 Mil-

lionen Dollar von Banken an Geldautomaten zu erbeuten. In sieben deutschen Städten erlangten die Betrüger 1,8 Millionen Euro. Als man einige Bandenmitglieder in Manhattan beobachtete, wie sie von Geldautomat zu Geldautomat zogen und Geld abhoben, waren ihre Rucksäcke mit Dollarscheinen prall gefüllt. Allein in New York City zogen sie aus 2904 Geldautomaten 2,4 Millionen Dollar. Die Beute von insgesamt 45 Millionen Dollar (= etwa 34 Mio. Euro) ist die bisher höchste Summe, die bei einem derartigen organisierten Cyber-Bankraub zusammenkam, so die New Yorker Staatsanwältin Loretta Lynch, als sie die Verhaftung von sieben Bandenmitgliedern in New York bekannt gab: „Das war Bankraub im Stil des 21. Jahrhunderts, der mithilfe des Internets ausgeführt wurde und um den gesamten Globus reichte".

Die Bande waren über das Internet in die Rechner einer indischen Firma eingedrungen, die für Kunden weltweit Zahlungsdienstleistungen erledigt. Dort stahlen sie die elektronisch gespeicherten Daten für Prepaid-Debitkarten einer Bank aus den Vereinigten Arabischen Emiraten. Zudem setzten sie bei ihrem digitalen Einbruch das Limit der Karten hoch. Danach schickten sie die Informationen über das Netz an Fußsoldaten in aller Welt. Diese programmierten mit einfach zu bekommenden Geräten die Magnetstreifen beliebiger Karten neu und hoben damit massenhaft Geld ab. Um die Spur zu verwischen, kauften Mitglieder dieser Gangs teure Autos oder Schmuck. Sieben von ihnen wurden festgenommen, ein weiteres Mitglied wurde erschossen aufgefunden. Alle stammen aus der Dominikanischen Republik und wohnten in der Nähe von New York. Die Aktion hat den US-Ermittlern zufolge schon im Oktober 2012 begonnen; damals erbeuteten die Cyber-Kriminellen etwa fünf Millionen Dollar. Durch den Erfolg ermutigt, stahlen die Hacker im Februar 2013 erneut Kartendaten einer Bank aus dem Nahen Osten und sackten diesmal über ihre Mittelsmänner 40 Millionen Dollar ein. Die Teams hoben dafür in etwa zehn Stunden weltweit 36.000-mal Geld ab.

Auch in Deutschland waren die Betrüger unterwegs. Ralf Herrenbrück, Sprecher der Staatsanwaltschaft Düsseldorf: „An Geldautomaten in sieben Orten in West-, Nord- und Süddeutschland wurden insgesamt 2,4 Millionen US-Dollar (1,8 Millionen Euro) von einem Konto der Bank aus dem Nahen Osten abgehoben." Zwei Täter wurden von der Polizei festgenommen, als sie in Düsseldorf mit manipulierten Karten 169.000 Euro abhoben. Ein Bankkunde beobachtete, wie sie vermummt und in Eile den Vorraum einer Bank verließen, und informierte die Polizei. Diese fand die Täter und ihre Beute in einem Auto, das in der Nähe abgestellt war. Bei den Tätern handelt es sich um einen 35 Jahre alten Mann und eine 56 Jahre alte Frau aus den Niederlanden. Eine dritte Person befindet sich dort in Auslieferungshaft. Die Staatsanwaltschaft Düsseldorf koordiniert derzeit die weiteren strafrechtlichen Ermittlungen zu dem Fall in Deutschland. Dabei geht es unter anderem um etwaige Hintermänner.

Die „Deutsche Kreditwirtschaft", eine Organisation, in der alle deutschen Banken zusammengeschlossen sind, verwies darauf, dass alle 94 Millionen EC-Karten (Girocards) in Deutschland seit Herbst 2012 mit einem fälschungssicheren Chip ausgerüstet sind, ebenso alle 60.000 Geldautomaten und alle 750.000 Terminals im Handel. Der Chip habe den Magnetstreifen abgelöst. Alle Abhebungen von Geldautomaten in Deutschland funktionieren ausschließlich über den Chip. Der Magnetstreifen ist zwar weiter auf der Karte vorhanden, über ihn laufen aber nur Funktionen wie der Kontoauszugsdrucker. Dadurch seien betrügerische Transaktionen mittels Kartendubletten im deutschen Girocard-System ausgeschlossen. Dass in sieben deutschen Orten mit manipulierten Karten Geld abgehoben wurde, liegt daran, dass offenbar nicht EC-Karten, sondern Dubletten von Prepaid-Karten des US-Kreditkartenunternehmens Mastercard genutzt wurden, für die der Magnetstreifen auch noch bei deutschen Geldautomaten funktioniert. Da es sich bei den gestohlenen Informationen um Konten für Guthabenkarten handelte, wurden keine Bankkunden geschädigt, sondern nur die Banken selbst. Dies ist auch der Grund, weshalb es länger gedauert hat, bis der digitale Bankraub bemerkt wurde. Die Art des Bankraubs mithilfe von Datendiebstahl ist nicht neu. 2007 nahmen Ermittler des FBI einen Mann namens Max Butler fest, der unter dem Pseudonym Iceman Kreditkartendaten gestohlen und weiterverkauft hatte. Die Daten hatte er sich über das Internet zum Beispiel von den schlecht gesicherten Rechnern einer Pizza-Kette geholt (Freiberger/Martin-Jung, „Krimineller Flashmob", SZ 11./12.05.2013, 1, 12).

Kirgisien

Deutsche Entwicklungshilfe beim Bespitzeln

Das Bundeskriminalamt (BKA) hat die kirgisische Regierung mit deutscher Überwachungstechnik ausgestattet und Sicherheitsbehörden damit vertraut gemacht. In den Jahren 2008 bis 2012 führte das BKA in Kirgisien drei Lehrgänge unter anderem für Mitglieder des Staatskomitees für Nationale Sicherheit und des kirgisischen Innenministeriums durch. Darin ging es nach offiziellen Angaben des BKA unter anderem um die „Ortung von Mobiltelefonen, den Einsatz der stillen SMS, die Funkzellenauswertung und auch die Online-Durchsuchung". In Kirgisien sind 2010 bei Unruhen schätzungsweise 2.000 Menschen ums Leben gekommen. Menschenrechtsorganisationen wie Human Rights Watch warfen den Sicherheitsbehörden der ehemaligen Sowjetrepublik willkürliche Verhaftungen und Folter vor. Das BKA bestätigte, dass es das kirgisische Staatskomitee für Nationale Sicherheit ein Jahr zuvor mit einem VW-Transporter, einer Video-Observationsanlage, einem Scanner und einem Mobiltelefon „für insgesamt 73.200 Euro" ausgestattet hat. Bundestagsabgeordnete kritisieren die Kooperation. Ulla Jelpke, die innenpolitische Sprecherin der Linken, erklärte: „Deutschland gibt dem kirgisischen Regime die Mittel in die Hand, die Opposition zu bespitzeln und zu unterdrücken." Der Vorgang zeige, „dass die parlamentarische Kontrolle solcher Ausbildungs- und Ausstattungshilfe dringend verbessert werden muss" (Nachhilfe beim Bespitzeln, Der Spiegel 14/2013, 13).

Technik-Nachrichten

Rüstungskonzern entwickelt Netzwerk-überwachungs-Tool

Der US-Rüstungszulieferer Raytheon hat eine Software zur Auswertung von Profilen in sog. sozialen Netzwerken entwickelt, mit der der Tagesablauf und soziale Kontakte und Beziehungen von Zielpersonen analysiert werden können. Der Rüstungskonzern verdient ansonsten sein Geld mit Marschflugkörpern, Torpedos und Radarsystemen. Der „Guardian" hat ein Werbevideo des Unternehmens aus dem Jahr 2010 veröffentlicht, das eine Überwachungs-Software demonstriert. Das dabei vorgeführte Raytheon-Programm Riot (eine Abkürzung für Rapid Information Overlay Technology) verknüpft öffentlich zugängliche Informationen zu einer Person aus Netzwerken wie Facebook, Twitter und Foursquare. Das Programm speichert Positionsdaten und liest sie auch aus den Metadaten publizierter Fotos aus. Die Ortsangaben werden analysiert, die Software zeigt dann zum Beispiel, wie oft und zu welchen Zeiten eine Person an bestimmten Orten ist. Außerdem rekonstruiert das Programm Kontaktnetzwerke aus den bei Twitter und Facebook zugänglichen Informationen.

Bei einem normalen Tagesablauf kann man so mit gewisser Wahrscheinlichkeit vorhersagen, wer wann wo anzutreffen sein dürfte. Der Raytheon-Mitarbeiter, der in dem Video das Programm vorführt, beschreibt den möglichen Einsatz so: „Wenn Sie Nick treffen wollen oder Zugriff auf sein Laptop brauchen, wäre Montagmorgen 6 Uhr im Fitnessstudio die beste Zeit dafür." Nach eigenen Angaben hat Raytheon die Software bislang nicht verkauft. Ähnliche Programme haben schon andere Firmen wie z. B. HBGary im Angebot. Auch die Schufa wollte öffentlich zugängliche Daten auf Facebook und Twitter nutzen, um die Kreditwürdigkeit von Menschen zu prüfen, zog die Pläne aber nach öffentlichen Protesten zurück (Raytheon: US-Rüstungsfirma erprobt Facebook-Überwachung, www.spiegel.de 11.02.2013)

Schweden

Memoto entwickelt Lif-Log-Kamera

Die schwedische Firma Memoto in Stockholm, ein 2012 gegründetes Start-up mit 17 festen Mitarbeitenden aus Schweden, Singapur und den USA, entwickelt eine Minikamera mit Datenspeicherung, welches als Gedächtnis der Nutzenden dienen und den Blick auf diese verändern soll. Die Kamera ist so winzig wie eine Streichholzschachtel. Die Memeto-Kamera kann mit einem Clip an der Kleidung befestigt oder an einer Kette um den Hals getragen werden. Sie macht automatisch alle 30 Sekunden ein Bild, 120 Bilder pro Stunde, 2880 am Tag. Zu jedem Bild speichert das Gerät die Uhrzeit und per GPS den Ort, womit ein riesiges Fototagebuch erstellt wird, ein „Life Log". Die Bilder werden auf den Servern von Amazon übertragen, das diese für Memoto speichert. Die Memoto-Software sortiert die Fotos, ordnet sie nach Motiven und Zeiten und markiert die technisch gelungensten. Der oder die Nutzende kann die Bilder über ein Smartphone abrufen, weiter bearbeiten oder z. B. über Facebook posten. Die Memoto-Kamera ist immer aktiv; sie lässt sich nur dadurch stoppen, dass sie in die Tasche gesteckt wird.

Martin Källström, Gründer von Memoto ist nicht der erste, der Life Logs entwickelt. Der kanadische Erfinder Steve Mann oder der Microsoft-Manager Gordon Bell experimentierten schon viele Jahre früher mit Geräten, die ihre Sinneseindrücke möglichst für immer bewahren sollten. Memoto will daraus ein Massengeschäft machen - sozusagen die totale Erinnerung für Jedermann. Ein bisschen appelliert Källström, die Privatsphäre anderer zu achten: „Respektiert, dass andere Menschen manchmal nicht fotografiert werden möchten". Doch das sei „Sache der Nutzer". Memoto habe keinen Zugriff aber die Daten, ebenso wenig die Werbeindustrie. Das Geld soll durch den Verkauf der Kameras verdient werden. Für 279 Dollars kann ein Exemplar reserviert werden; Auslieferung noch im Jahr 2013. Einer der Vorbilder ist für Memoto Instagram, das auch mit zwölf Mitarbeitenden anfing und 2012 von Facebook für eine Milliarde Dollar übernommen wurde. Instagram änderte danach für einige Monate vorübergehend seine Geschäftsbedingungen und lies sich umfassende Nutzungs- und Verwertungsrechte an den Fotos der Nutzenden einräumen (Wolf, Totale Erinnerung, Der Spiegel 18/2013, 111).

Die psychologischen Folgen der Beschäftigten-überwachung

Im Fachmagazin „Journal of Applied Psychology" beschäftigen sich WissenschaftlerInnen um die US-Psychologin Lori Foster Thompson mit dem Monitoring von speziellen Arbeitsabläufen am Arbeitsplatz und stellen ihre Studie „When Big Brother Is Watching" vor. Das Forschungsteam von der North Carolina State University untersuchte, welche Effekte es hat, wenn während eines Online-Trainings alle Lernschritte und Lernerfolge der MitarbeiterInnen von einer Computersoftware mit erfasst werden. Dies sind oft genau die Dinge, die Vorgesetzte interessieren: Führt ein Training zum gewünschten Lernerfolg? Lässt sich erhöhte Produktivität messen?

Kontrolle am Arbeitsplatz ist regelmäßig mit einer negativen Assoziation verbunden. Schlagzeilen, die dieses Gefühl bei vielen angestellt Arbeitenden unterfütterten, lieferte in den vergangenen Jahren die systematische verdeckte Überwachung von MitarbeiterInnen in vielen Unternehmen, etwa beim Lebensmittel-Discounter Lidl, der Telekom und der Deutschen Bahn. Doch ist die Kontrolle am Arbeitsplatz nicht immer darauf ausgerichtet, Mitarbeiter beim Diebstahl zu erwischen oder andere Anhaltspunk-

te für korruptes Verhalten zu finden. Das Dilemma des Monitoring ist, dass es für den Arbeitgeber wichtige Informationen liefern kann, von den ArbeitnehmerInnen aber oft als Bedrohung empfunden wird.

Das Ergebnis der Studie ist ernüchternd: Die TeilnehmerInnen des Schulungsprogramms wurden angespannter, wenn sie vom Monitoring wussten – und dadurch wiederum auch schlechter, und zwar allesamt. Einige MitarbeiterInnen fanden das Monitoring belastender, wenn es „live“, also in Echtzeit stattfand, andere mehr, wenn es zeitversetzt erfolgte. Gut für den Lernerfolg war es in keinem der Fälle.

Ein ähnliches Ergebnis hatte bereits eine der ersten Studien zu diesem Thema gefunden. Im Fachmagazin „Research Contributions“ berichtete ein Forschungsteam aus Kanada schon 1986, dass sich computergestütztes Monitoring von Arbeitsabläufen negativ auswirken kann. Bei der Untersuchung von Versicherungsunternehmen und staatlichen Institutionen hatten die WissenschaftlerInnen festgestellt, dass eine computergestützte Überwachung der Produktivität – etwa, wie viele Versicherungsfälle pro Tag jemand bearbeitete – zu erhöhter Ängstlichkeit und Ärger bei den Angestellten führte. Damit einher ging eine sinkende Arbeitszufriedenheit und geringere Motivation und Eigeninitiative. Die Produktivität im Sinne der Quantität stieg jedoch durch das Monitoring. Durchschnittlich wurden mehr Versicherungsfälle pro Tag bearbeitet; die Qualität der Arbeit wurde dabei aber nicht erfasst. Für ArbeitspsychologInnen stellt sich aus diesen Befunden die Frage, ob nicht beides vereinbar wäre: eine erhöhte oder verbesserte Leistung durch Monitoring – ohne dass dadurch das Wohlbefinden des Mitarbeiters geschmälert wird.

Tim Hagemann, Arbeitspsychologe an der Fachhochschule der Diakonie in Bielefeld, meint, dass der Ton die Musik macht: „Welchen Effekt Monitoring auf einen Mitarbeiter hat, hängt davon ab, ob die Maßnahme als bloße Kontrolle oder als Unterstützung, etwa zur Verbesserung von Arbeitsabläufen, wahrgenommen wird.“ Monitoring sei im Grunde nichts anderes als eine Rückmeldung darüber, was im Arbeitsalltag gut oder schlecht laufe. „Jeder braucht im Arbeitsalltag Feedback und Rückmeldungen – ohne sie würden wir sonst im luftleeren Raum agieren.“ Entscheidend sei, wie die Führungskraft das Monitoring vermittelt und wie empfindsam die jeweilige MitarbeiterIn sei. „Monitoring kann als konstruktives Feedback, Absicherung, Verunsicherung oder purer Stressor empfunden werden – die Grenzen sind fließend.“ Wie eine solche Maßnahme bei MitarbeiterInnen ankommt, hängt auch stark von dem Verhältnis ab, das MitarbeiterInnen und Vorgesetzte zueinander haben. Wird der Chef als fachlich kompetent eingestuft und traut man ihm eine angemessene Einschätzung der eigenen Arbeit zu, dann kann man Monitoring-Maßnahmen auch besser annehmen. Hätte etwa die Studie von Lori Foster Thompson nicht nur den Lernerfolg gemessen, sondern integrierte Unterstützungsfunktionen gehabt, wäre das Ergebnis vielleicht anders ausgefallen.

Es scheint gar nicht so schwierig zu sein, Monitoring so zu gestalten, dass es auch als unterstützend oder absichernd empfunden werden kann. Eine Ausnahme, so Hagemann, sei die Videoüberwachung: „Wenn eine Kamera mich während der gesamten Arbeitszeit filmt, ist das keine angenehme Grundsituation.“ Denn dann werden nicht nur Arbeitsabläufe kontrolliert, sondern jedes Verhalten überwachbar gemacht – und das erzeugt Stress. „In meiner Forschung nutze ich eine Kamera im Experiment oft genau dazu: um Stress auszulösen. Und wenn man Menschen stresst, leidet nicht nur die Leistung. Es steigt auch das Risiko, dass Konflikte zwischen den Mitarbeitern zunehmen.“ Das fand auch die Studie der kanadischen WissenschaftlerInnen heraus: Die überwachten MitarbeiterInnen gaben an, dass sich ihre Arbeitsbeziehungen verschlechterten, und zwar nicht nur die zu den Vorgesetzten, sondern auch die Beziehungen zu anderen KollegInnen.

Aus der sozialwissenschaftlichen Forschung ist seit längerer Zeit bekannt, dass zu starke Kontrolle Frustration, Angst und Aggression schürt. Diese muss irgendwohin. In der Regel wandert sie in den Körper – der Ärger wird im wahrsten Sinne des Wortes „geschluckt“. Der Körper reagiert darauf, indem er Stresshormone ausschüttet und den Blutdruck sowie die Herzrate erhöht. Außerdem wird das Immunsystem heruntergefahren, um Energie für die stressreiche Situation zu sparen. Kommt zu diesen Faktoren noch äußere Unsicherheit, etwa durch die Angst vor Arbeitsplatzverlust, wird zusätzlich mehr gemobbt; die Aggression wird offener ausgelebt. Zu viel Kontrolle kann je nach Bewältigungsstrategie so dazu führen, dass MitarbeiterInnen auf Dauer körperlich oder psychisch krank werden, sich in die innere Kündigung zurückziehen oder aufeinander herumhacken.

Die damit in Gang gesetzte unheilvolle Spirale nennt der Psychologe Oliver Sträter von der Universität Kassel „Lidl-Effekt“: Durch den Rückzug der MitarbeiterIn wächst das Misstrauen des Chefs, der wiederum die Kontrolle verstärkt. So steigt der Druck auf beiden Seiten: „Führen wird oft mit Kontrolle verwechselt.“ Viele würden die Loyalität ihrer MitarbeiterInnen unterschätzen. Tim Hagemann hält Führung durch Kontrolle höchstens kurzfristig für sinnvoll. Langfristig sei das keine gute Idee (Jimenez, Diese Vorteile bietet Überwachung von Mitarbeitern, www.welt.de 19.03.2013).

Gesundheitssensoren - auf die Haut aufgedruckt

Ein Forschungsteam im Labor des Materialwissenschaftlers John Rogers an der University of Illinois in Urbana-Champaign/USA hat sogenannte „epidermal electronics“ entwickelt, die sich wie entfernbare Tattoos auf die Körperhaut aufbringen lassen (vgl. DANA 1/2012, 40). Das Verfahren erlaubt es den Nutzenden, Gesundheitssensoren ständig zu tragen, ohne dass sie bei Alltagsaktivitäten stören. Mit der Technik kann beispielsweise der Wundheilprozess nach chirurgischen Eingriffen überwacht werden. Das Prototypsystem besteht aus ultradünnen Elektroden, Sensorik, einer drahtlosen Stromversorgung sowie passender Kommunikationstechnik. Die Forschenden hatten zunächst mit einem dünnen Elastomer gearbeitet, auf dem die flexiblen Komponenten aufgebracht waren. Rogers

erläuterte: „Für den Normalbetrieb in geschlossenen Räumen war das ausreichend. Beim Duschen oder Schwimmen würde es wohl nicht halten“. Aus diesem Grund entwickelten der Materialwissenschaftler und seine KollegInnen das direkte Druckverfahren, das den Gesundheitsmonitor deutlich haltbarer macht: „Wir fanden heraus, dass man den Elastomerrücken gar nicht benötigt. Man kann ein Stempelverfahren nutzen, um das Netz aus Elektronik direkt auf die Hautoberfläche zu bringen.“

Bereits kommerziell erhältliche Sprühpflastersysteme können genutzt werden, um die Sensorik mit einer zusätzlichen Schutzschicht zu versehen. Damit wird der Gesundheitsmonitor zudem enger mit der Haut verknüpft. Ohne den Elastomerrücken sei das System sehr robust und auch deutlich dünner; es passt sich der Hautoberfläche besser an. Das aktuelle Prototypsystem hält immerhin bis zu zwei Wochen, bevor die natürlichen Hauterneuerungsprozesse dafür sorgen, dass es sich langsam auflöst. Während der zwei Wochen kann das Gerät Werte wie Temperatur, ausgeübte Kräfte oder den Feuchtigkeitsstatus der Haut erfassen, voraus sich dann wiederum Einblicke in den weiteren Gesundheitszustand der TrägerIn ergeben. Zur Überwachung der Wundheilung bringt ein Arzt das System neben einer Operationswunde an, bevor die PatientIn das Krankenhaus verlässt. Über die nächsten Wochen kann danach erfasst werden, wie sich die Wunde entwickelt – inklusive drahtloser Rückmeldung an das Krankenhaus. Eine kommerzielle Nutzung ist noch nicht geplant. Rogers‘ Labor arbeitet daran, Stromversorgung und Funkeinheit zu verbessern. Vermarktet werden könnte der Gesundheitsmonitor über das Start-up MC10, eine von Rogers mitgegründete Spezialfirma für flexible Elektronik (Orcutt, Elektronische Tattoos, www.heise.de 27.03.2013).

Rechtsprechung

BGH

Keine Beeinträchtigung der gerichtlichen Presseberichterstattung

Der Bundesgerichtshof entschied mit Urteil vom 19.03.2013, dass die Presse über in öffentlicher Verhandlung erörterte Details berichten darf, selbst, wenn damit die Intimsphäre der Betroffenen tangiert wird (Az. VI ZR 93/12). Auch in einem Zivilverfahren kann der Presse insofern kein Schreibverbot erteilt werden. Der Kläger Jörg Kachelmann war bis zu seiner Verhaftung im März 2010 wegen des Verdachts der Vergewaltigung einer damaligen Freundin als Fernsehmoderator und Journalist tätig. Er wendet sich mit seinem Unterlassungsbegehren gegen eine ihn betreffende Online-Berichterstattung auf dem von der Beklagten betriebenen Internetportal „www.bild.de“ während eines gegen ihn geführten Strafverfahrens.

Kurz nach seiner Verhaftung begann eine intensive Medienberichterstattung über das gegen ihn wegen schwerer Vergewaltigung und gefährlicher Körperverletzung eingeleitete Strafverfahren sowie über sein bis zu diesem Zeitpunkt der breiten Öffentlichkeit unbekanntes Privatleben, insbesondere seine Beziehungen zu Frauen. Durch inzwischen rechtskräftiges Urteil wurde er von den Tatvorwürfen freigesprochen. Das Protokoll über Kachelmanns Aussage beim Untersuchungsrichter wurde später auch im Prozess verlesen. Schon vor Prozessbeginn hatte das Nachrichtenmagazin „Focus” aus einer Vernehmung Kachelmanns vor dem Untersuchungsrichter berichtet. In dieser Aussage schilderte Kachelmann, dass in der angeblichen Tatnacht seine damalige Freundin mit Sado-Maso-Utensilien auf ihn gewartet habe. Über diesen „Focus”-Artikel berichtete wiederum „BILD.de” am 13.06.2010.

Das Landgericht hat die Beklagte verurteilt, es zu unterlassen die beanstandeten Äußerungen, aus denen sich Rückschlüsse auf die sexuellen Neigungen des Klägers ergaben, wie in dem Artikel vom 13.06.2010 zu veröffentlichen oder sonst zu verbreiten. Das Oberlandesgericht (OLG) Köln hatte die Berufung der Beklagten am 14.02.2012 zurückgewiesen und der Klage Kachelmanns gegen „Bild.de” stattgegeben. Nach Auffassung des OLG Köln hätte die Presse selbst nach der Verlesung seiner Aussage nicht berichten dürfen, weil die Medienöffentlichkeit wesentlich größer sei als die Saalöffentlichkeit im Gerichtssaal. Auf die Revision der Beklagten hat der für den Schutz des allgemeinen Persönlichkeitsrechts zuständige VI. Zivilsenat des BGH die Unterlassungsklage abgewiesen. Wegen der aus dem Rechtsstaatsprinzip (Art. 20 Abs. 3 Grundgesetz) folgenden und in Art. 6 Abs. 2 der europäischen Menschenrechtskonvention anerkannten Unschuldsvermutung und einer möglichen durch die Medienberichterstattung bewirkten Stigmatisierung war die Veröffentlichung im Juni 2010 wegen einer Verletzung des Persönlichkeitsrechts des Klägers rechtswidrig. Ein Unterlassungsanspruch des Klägers besteht nach Ansicht des BGH dennoch nicht. Nach Verlesung des Protokolls über seine haftrichterliche Vernehmung in der öffentlichen Hauptverhandlung sei eine aktuelle Prozessberichterstattung unter Einbeziehung der beanstandeten Äußerungen zulässig gewesen. Infolgedessen sei die für den Unterlassungsanspruch erforderliche Wiederholungsgefahr entfallen (BGH, PM v. 19.03.2013; Kachelmann-Klage gegen Prozessberichterstattung abgewiesen, www.bild.de 19.03.2013).

OLG Köln

ZKA durfte DigiTask-Software nicht einsetzen

Das Oberlandesgericht (OLG) Köln hat mit Beschluss vom 22.03.2013 das Zollkriminalamt (ZKA) für den Einsatz einer Analysesoftware gerügt, mit der Daten aus einer Überwachungsmaßnahme im Jahr 2011 ausgewertet wurden (Az. 16 Wx 16/12). Zwölf Tage lang waren Telefongespräche eines Verdächtigen abgehört und der Internetverkehr mitgeschnitten worden, gleichzeitig wurde ein Strafverfahren gegen den Verdächtigen eingeleitet. Während die Telefondaten nach der Überwachung gelöscht worden waren, blieben die Internetdaten noch über ein Jahr lang auf den Rechnern des ZKA gespeichert - darunter auch E-Mails, die der Verdächtige mit seinem Verteidiger ausgetauscht hatte. Deswegen hatte der Überwachte Beschwerde eingelegt.

Das Gericht stellte fest, dass die Kommunikation mit einem Anwalt rechtlich besonders geschützt ist. Wenn derartige E-Mails oder Telefongespräche bei einer Überwachung aufgezeichnet werden, müssen diese umgehend gelöscht werden. Das ZKA hatte jedoch offenbar eine alte Version einer „TKÜ-Auswertsoftware“ des Herstellers DigiTask im Einsatz, mit dem das Löschen bestimmter Kommunikationsvorgänge im Datenstrom nicht möglich war. DigiTask hatte das ZKA in einem Schreiben selbst auf eine neue Softwareversion mit eben dieser Möglichkeit hingewiesen, deren Einsatz rechtlich geboten sei. Allerdings hätte die Behörde dafür wohl einen leistungsfähigeren Server mit neuem Betriebssystem benötigt. Mit der alten Software gab es nur die Optionen, alles oder gar nichts aufzubewahren; das ZKA entschied sich für alles, was vom OLG beanstandet wurde: „Probleme bei der Beschaffung der erforderlichen Hard- und Software rechtfertigen keinen Grundrechtseingriff.“ Die technische Ausstattung müsse den Vorgaben der Gesetze und des Grundgesetzes entsprechen. Insofern sei die Überwachung rechtswidrig gewesen (Zollkriminalamt für Einsatz von DigiTask-Software abgewatscht, www.spiegel.de, 10.04.2013; openjur.de/u/620970.html).

LG Duisburg

Kein Zeugnisverweigerungsrecht bei selbsteingestellten Online-Beiträgen

Die 2. große Strafkammer des Landgerichts (LG) Duisburg hat April 2013 entschieden, dass ein 33jähriger Redakteur des Bewertungsportals über Kliniken MedizInfo für höchstens 5 Tage in Beugehaft muss, weil er die Identität eines Internetnutzers nicht aufdecken will, der online diffamierend über eine Ärztin geschrieben hat. Er hat Verfassungsbeschwerde gegen die Entscheidung des LG Duisburg eingelegt.

Ein Beitrag in dem Internet-Portal, mit dem einer Ärztin in einem westfälischen Krankenhaus mehr sexuelles als berufliches Interesse an ihren Patienten unterstellt wurde, löste 2011 Ermittlungen der Staatsanwaltschaft Dortmund wegen übler Nachrede gegen „Unbekannt“ aus. Der Redaktuer weigert sich hartnäckig, den Namen des Verfassers zu nennen.

Schon das Amtsgericht (AG) hatte entschieden, dass er nicht als Journalist einzustufen sei, und belegte ihn zunächst mit einem Ordnungsgeld in Höhe von 50 Euro, ersatzweise einem Tag Haft. Der Redakteur legte dagegen Beschwerde ein, ebenso gegen den späteren Beschluss, der ihm Beugehaft androhte. Das LG wies die Beschwerden ab. Es stellte nicht in Frage, dass er Mitarbeiter des Portals sein, womit er sich prinzipiell auf das Journalisten strafprozessrechtlich zugesicherte Zeugnisverweigerungsrecht berufen könne. Dies gelte aber nicht für den konkreten Fall: Ein Beitrag in einem Internetportal, den der Nutzer ungefiltert selbst einstellt, sei nicht dem redaktioneller Kontrolle unterliegenden Leserbrief in einer Tageszeitung gleichzusetzen. Ins Gefängnis wird der Redakteur nicht gehen. Er kündigte an, den Namen preiszugeben (Malsch, Online-Redakteur muss wegen Aussageverweigerung in Beugehaft, www.derwesten.de 03.05.2013; LG Duisburg: Online-Redakteur muss wegen unterlassener Preisgabe eines Usernamens in Beugehaft, beck-aktuell.beck.de 06.05.2013; ebenso LG Augsburg, B.v. 19.03.2013, AfP 2013, 159; Janisch, Privileg der Presse, SZ 07.05.2013, 31).

LG Augsburg

Durchsuchungsanordnung bei Redaktion war rechtswidrig

Das Landgericht (LG) Augsburg stellte mit Beschluss vom 19.03.2013 in einem Beschwerdeverfahren fest, dass Beleidigung im Internet kein Grund für eine Durchsuchung einer Redaktion ist und hob einen Beschluss des Amtsgerichtes (AG) Augsburg auf (Az. x Qs 151/13). Ein CSU-Referent hatte sich von einem Nutzer im Online-Forum der „Augsburger Allgemeinen“ beleidigt gefühlt. Das AG hatte auf dessen Initiative hin angeordnet, die Daten des Nutzers zu beschlagnahmen und hierfür die Durchsuchung der Redaktion angeordnet.

Die Polizei hatte am 28.01.2013 bei dem Verlag die persönlichen Daten eines Internetforumnutzers beschlagnahmt. Hintergrund war eine Strafanzeige des Augsburger Ordnungsreferenten Volker Ullrich (CSU), der sich beleidigt sah. Journalistenverbände hatten die Aktion scharf kritisiert und von einem überzogenen Vorgehen gesprochen. Ullrich, selbst Volljurist, fühlte sich durch folgenden Forenkommentar verunglimpft: „Dieser Ullrich verbietet sogar erwachsenen Männern ihr Feierabendbier ab 20.00 Uhr, indem er geltendes Recht beugt und Betreiber massiv bedroht!“ Der Forennutzer hatte mit diesen Worten kritisiert, dass Ordnungsreferent Ullrich gegen den Verkauf von Alkohol an Tankstellen nach 20 Uhr vorgegangen war.

Zu einer Durchsuchung der Redaktion war es zwar nicht gekommen, weil die Zeitung die Daten der Polizei übergab, um die drohende Durchsuchung zu verhindern. Die Richter des LG bemängelten nun, dass das AG gar keine Anordnung zur Durchsuchung der Räume und Beschlagnahme der Daten hätte erlassen dürfen, da die Äußerungen des Users, durch die sich der Referent beleidigt fühlte, bei einer Gesamtbetrachtung als nicht strafbar anzusehen sei. Die Kritik an Ullrich stelle „lediglich eine subjektive Bewertung der Haltung des Ordnungsreferenten dar, auch wenn diese

Bewertung in herabwürdigender Form erfolgte". Nach der Rechtsprechung des Bundesverfassungsgerichts sei bei Äußerungen zu politischen Themen in der Öffentlichkeit der straffreie Bereich im Hinblick auf die Meinungsfreiheit weiter zu fassen als bei Äußerungen in der Privatsphäre.

Stoff für weitere Diskussionen wird folgende presserechtliche Aussage des LG abgeben: „Forum-User genießen nicht den Schutz der Pressefreiheit." Userbeiträge seien nicht dem redaktionellen Bereich zuzuordnen, Forum-User seien nicht als Informanten eines Pressemitarbeiters anzusehen. Die Verantwortung für derartige Beiträge liege nach den Nutzungsbestimmungen des Forums allein beim jeweiligen Nutzer, von deren Inhalt sich die Betreiberin ausdrücklich distanziere (Beschlagnahme bei der „Augsburger Allgemeinen": Anordnung der Durchsuchung war rechtswidrig, www.spiegel.de 20.03.2013; Mayr, Durchsuchung bei Zeitung rechtswidrig, SZ 21.03.2013, 34; Urteil abzurufen unter http://www.justiz.bayern.de/imperia/md/content/stmj_internet/gerichte/landgerichte/augsburg/durchsuchung_von_presser_umen.pdf).

LG Berlin

Allgemeine Geschäftsbedingungen von Apple in wesentlichen Teilen rechtswidrig.

Der Verbraucherzentrale Bundesverband (vzbv) hat die Apple Sales International mit Sitz in Irland vor dem Landgericht Berlin wegen der Allgemeinen Geschäftsbedingungen im Internet-Apple Store verklagt. Das Landgericht Berlin hat den Verbraucherschützern mit Urteil vom 30.04.2013 (Gesch.Z.: 15 O 92/12) auf ganzer Linie Recht gegeben. Wir dokumentieren die wesentlichen Urteilsgründe des – nicht rechtkräftigen - Urteils, welches Folgen für alle Geschäfte des Apple Store mit Kundinnen und Kunden in Deutschland haben wird:

In dem Rechtsstreit Verbraucherzentrale Bundesverband e.V. … gegen die Apple Sales International … hat die Zivilkammer 15 des Landgerichts Berlin in Berlin - Mitte, … für Recht erkannt:

I. Die Beklagte wird verurteilt, es … zu **unterlassen,** nachfolgende oder mit diesen inhaltgleiche Bestimmungen in Verträge … über Leistungen mit Verbrauchern, die ihren gewöhnlichen Aufenthalt in der Bundesrepublik Deutschland haben, einzubeziehen, sowie sich auf die Bestimmungen bei der Abwicklung derartiger Verträge, geschlossen nach dem 17. Dezember 2009, zu berufen: …

3. (Erheben und nutzen von personenbezogenen Daten

Wenn Sie mit Apple oder einem mit Apple verbundenen Unternehmen in Kontakt treten, können Sie jederzeit dazu aufgefordert werden, personenbezogene Daten von Ihnen anzugeben.)

Apple und **seine verbundenen Unternehmen können diese personenbezogenen Daten untereinander austauschen und sie nach Maßgabe dieser Datenschutzrichtlinie nutzen.**

Sie können solche Daten auch mit anderen Informationen verbinden, um unsere Produkte, Dienstleistungen, Inhalte und Werbung anzubieten oder zu verbessern.

4. (Welche personenbezogenen Daten erheben wir)

Wenn du **Inhalte mit Familie oder Freunden teilst und dabei Produkte von Apple verwendest, Geschenkgutscheine und Produkte verschickst oder andere dazu einlädst, sich dir in einem Apple Forum anzuschließen, kann Apple die Daten erheben, welche du über diese Personen zur Verfügung stellst, wie Name, Adresse, E-Mail und Telefonnummer.**

5. (Wie wir personenbezogene Daten nutzen)

Die personenbezogenen Daten, die wir erheben, erlauben uns, dich über die neuesten Apple Produktankündigungen, Softwareupdates und anstehenden Veranstaltungen zu informieren.

Du hilfst uns auch damit, unsere Dienste, Inhalte und Werbung zu verbessern.

(Wenn du nicht in unserem Verteiler sein möchtest, kannst du dich jederzeit abmelden, indem du deine Einstellungen änderst.)

6. (Wie wir personenbezogene Daten nutzen)

Wir nutzen personenbezogene Daten auch als Unterstützung, um unsere Produkte, Dienste, Inhalte und Werbung zu entwickeln, anzubieten und zu verbessern.

7. (Wie wir personenbezogene Daten nutzen)

Wir können personenbezogene Daten auch für interne Zwecke nutzen, wie zur Datenanalyse und Forschung, um Apples Produkte, Dienste und die Kommunikation mit Kunden zu verbessern.

8. (Weitergabe an Dritte)

Mitunter wird Apple bestimmte personenbezogene Daten an strategische Partner weitergeben, die mit Apple zusammenarbeiten, um Produkte und Dienste zur Verfügung zu stellen, oder die Apple beim Marketing gegenüber Kunden helfen.

(Wenn du beispielsweise ein iPhone kaufst und aktivierst, ermöglichst du Apple und seinen Mobilfunkanbieter zum Austausch der Daten, die du während des Aktivierungsprozesses bereitstellst, um den Dienst zu ermöglichen. Wenn du für den Dienst zugelassen wirst, gelten die Datenschutzrichtlinien von Apple bzw. seinem Mobilfunkanbieter für deinen Account.) **Die personenbezogenen Daten werden von Apple** nur **weitergegeben, um** (unsere Produkte, Dienste oder) **unsere Werbung zu erbringen oder zu verbessern;** (sie werden nicht an Dritte für deren Marketingzwecke weitergegeben).

9. (Weitergabe an Dritte, Dienstleister)

Apple gibt personenbezogene Daten an Unternehmen weiter, die Dienstleistungen erbringen, wie zum Beispiel die Verarbeitung von Informationen, (Kreditgewährung, Ausführung von Kundenbestellungen, Lieferung von Produkten an dich), **Verwaltung und Pflege von Kundendaten,** (Erbringung eines Kundendienstes), **die Bewertung deines Interesses an unseren Produkten und Leistungen sowie das Betreiben von Kundenforschung oder die Durchführung von Umfragen zur Kundenzufriedenheit.**

10. (Standortbezogene Dienste)

Um standortbezogene Dienste auf Apple Produkten anzubieten, können Apple und unsere Partner und Lizenznehmer präzise Standortdaten erheben, nutzen und weitergeben, ein-

schließlich des geographischen Standorts deines Apple Computers oder Geräts in Echtzelt. Diese Standortdaten werden in anonymisierter Weise erhoben, durch die du nicht persönlich identifiziert wirst. **Diese werden von Apple und unseren Partnern und Lizenznehmern verwendet, um dir standortbezogene Produkte und dienste anzubieten und diese zu verbessern. Wir geben beispielsweise deinen geographischen Standort an Anwendungsdienstleister weiter wenn du deren Standortdienste auswählst.**

Der Kläger ist ein Verbraucherverband, der in die Liste der qualifizierten Einrichtungen gemäß § 4 UKIaG eingetragen ist. Die Beklagte vertreibt Computer-Hardware sowie Kommunikationsgeräte. Sie betreibt unter der Internetadresse www.apple.com einen Telemediendienst, der in deutscher Sprache unter www.apple.de erreichbar ist. Über den Telemediendienst www.apple.com/de hält die Beklagte „Geschäftsbedingungen", bezogen auf den „Apple Store" bereit, hinsichtlich deren Einzelheiten auf die Anlage K 1 Bezug genommen wird. Ferner hält sie auf einer Unterseite die „Apple- Datenschutzrichtlinie" bereit (Anlage K 2). Darin befinden sich die klägerseits beanstandeten, aus dem Tenor ersichtlichen Passagen. Der Kläger erblickt in der „Apple Datenschutzrichtlinie" Allgemeine Geschäftsbedingungen, die gegen § 307 Abs. 1 i. V. m, Abs. 2 Nr. 1 BGB, §§ 4, 4a BDSG; §§ 12, 13, 14 TMG; § 94 TKG; § 7 Abs. 2 UWG verstießen.

Soweit der Kläger zunächst angekündigt hat, weiter zu beantragen, die Beklagte zu verurteilen, folgende Klauseln zu verwenden:

1. **Am Ball bleiben! Haltet mich auf den Laufenden mit den aktuellen Apple Infos.** (Um zu erfahren, wie Apple Ihre persönlichen Informationen schützt, lesen Sie bitte die Datenschutz-Vereinbarung von Apple) soweit diese Einwilligungserklärung durch ein Häkchen bereits voreingestellt ist.

2. Am Ball bleiben! Haltet mich auf dem Laufenden mit den aktuellen Apple Infos. **Um zu erfahren, wie Apple Ihre persönlichen Informationen schützt lesen Sie bitte die Datenschutz-Vereinbarung von Apple**

haben die Parteien im Hinblick auf die beklagtenseits abgegebene strafbewehrte Unterlassungserklärung den Rechtsstreit übereinstimmend in der Hauptsache für erledigt erklärt und mit widerstreitenden Kostenanträgen verhandelt.

[Die Beklagte] sieht in den mit dem Klageanträgen zu 3. - 10. angegriffenen Bestimmungen, die Teil ihrer „Datenschutzrichtlinie" sind, keine Allgemeinen Geschäftsbedingungen, die in Verträgen zwischen ihr und deutschen Verbrauchern einbezogen würden. Die darin enthaltene Information von Verbrauchern sei nach den Bestimmungen der Richtlinie 95/46/EG (Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und im freien Datenverkehr) und dem insoweit anwendbaren irischen Recht erforderlich. Auch seien die Klageanträge zu unbestimmt, da im Falle einer Verurteilung unklar bliebe, welches Verhalten ihr zukünftig untersagt werden solle. Die klägerseits als „Allgemeine Geschäftsbedingungen" überreichte Anlage K 1 datiere vom 27. Juni 2011 und sei im Hinblick auf datenschutzrechtliche Aspekte zwischenzeitlich geändert worden. Die - insbesondere im Klageantrag zu 3, - angegriffenen Bestimmungen unterfielen nicht den Anforderungen des deutschen Datenschutzrechts, da sie keine personenbezogenen Daten durch eine Niederlassung in Deutschland erhebe. Auch liege keine unangemessene Benachteiligung i. S. d. § 307 Abs. 1 BGB vor, da für den durchschnittlichen Verbraucher erkennbar sei, dass den Bestimmungen der „Apple Datenschutzrichtlinie" keine rechtsgeschäftliche Bedeutung zukomme, sondern diese lediglich der allgemeinen Information über Datenerhebung, -Verarbeitung oder -nutzung ihrerseits dienten. Schließlich sei durch Abgabe einer strafbewehrten Unterlassungserklärung im Hinblick auf den angekündigten Antrag zu 2. auch die Wiederholungsgefahr hinsichtlich der übrigen Unterlassungsanträge entfallen….

[Aus den Entscheidungsgründen:] II. In der Sache hat die Klage Erfolg. Die klägerseits beanstandeten Bestimmungen verstoßen gegen § 307 Abs. 1 BGB. Insoweit ist hier hinsichtlich der Beurteilung der Gesetzeskonformität der Klauseln deutsches Recht maßgeblich. Gemäß Art. 6 ROM-I-VO - ist bei Verträgen, die ein Verbraucher mit einem Unternehmer schließt, das Recht des Staates maßgeblich, in dem der Verbraucher seinen gewöhnlichen Aufenthalt hat, soweit die Tätigkeit des Unternehmens auf irgendeine Weise auf den Heimatstaat des Verbrauchers ausgerichtet ist. Da die von der Beklagten verwendeten Allgemeinen Geschäftsbedingungen keine Rechtswahlvereinbarungen vorsehen, ist hinsichtlich deutscher Verbraucher deutsches Recht anwendbar. …

Entgegen der Auffassung der Beklagten handelt es sich - anders als in dem … Urteil der Kammer vom 26. Oktober 2012 - 15 O 449/09 -, in dem es um FAQ's ging, um Allgemeine Geschäftsbedingungen i. S. d. § 305 Abs. 1 S. 1 BGB. …

1. Klausel zu 3. (Erheben und Nutzen von personenbezogenen Daten) Die Klausel verstößt gegen § 307 Abs. 1 i. V. m. Abs. 2 Nr. 1 BGB, §§ 4, 4a BDSG; §§ 12, 13TMG. Sie differenziert nicht zwischen unterschiedlichen Datenbeständen. Umfasst sind also sowohl Daten, die der Verbraucher im Rahmen eines Bestellprozesses übermittelt, als auch die Daten der Nutzung eines Telemediendienstes. Sie stellt damit eine globale Einwilligung in Datenverarbeitungsprozesse dar, ohne dass der Umfang der Einwilligung dem Verbraucher hinreichend transparent gemacht wird (§ 4a BDSG).

Klausel zu 4. (Welche personenbezogenen Daten erheben wir) Auch diese Bestimmung verstößt gegen § 307 Abs. 1 i. V. m. Abs. 2 Nr. 1 BGB, §§ 4, 4a BDSG; §§ 12, 13, 14 TMG. Die Klausel benennt den Zweck der Erhebung nicht. Es wird keine Auskunft darüber erteilt, wie die Daten von der Beklagten genutzt werden. Sie führt zu einer Einwilligung zulasten Dritter. Dies führt dazu, dass der betroffene Verbraucher entgegen § 4a BDSG entgegen dem Gesetzeszweck weder eine bewusste noch eine „ohne jeden Zweifel" erfolgte Erklärung hinsichtlich der Datenverwendung abgibt Die Klausel erweckt zudem den Eindruck, als sei die Erhebung der Daten durch die Einwilligung des erklärenden Verbrauchers legitimiert. Dies führt dazu, dass der betroffene Verbraucher u. U. von der Geltendmachung ihm zustehender Rechte absieht.

Klausel zu 5. (Wie wir personenbezogene Daten nutzen) Auch diese Klausel verstößt gegen § 307 Abs. 1 i. V. m. Abs 2 Nr. 1 BGB, §§ 4, 4a BDSG; §§ 12, 13 TMG. Sie stellt eine Pauschaleinwilligung dar. Eine gesonderte Erklärung hinsichtlich des genannten Zweckes ist bei der vorliegenden Klausel nicht vorgesehen. Sie erweckt den Eindruck einer zwingenden, nicht zu verhindernden Einwilligung seitens des Verbrauchers.

Klausel zu 6. (Wie wir personenbezogene Daten nutzen - Teil 2 -) Auch diese Klausel verstößt gegen § 307 Abs. 1 i. V. m. Abs. 2 Nr. 1 BGB, §§ 4, 4a BDSG; §§ 12, 13 TMG. Die Klausel bezieht sich auf wörtliche Zwecke der Beklagten, ohne eine Auskunft darüber zu geben, welche der vom Verbraucher erhobenen Daten genutzt werden und wie dies im Einzelnen erfolgen soll. Auch insoweit wird der Verbraucher über die Möglichkeit der Verhinderung der Einwilligung getäuscht.

Klausel zu 7. (Wie wir personenbezogene Daten nutzen - Teil 3 -) Auch diese Klausel verstößt gegen § 307 Abs. 1 i. V. m. Abs. 2 Nr. 1 BGB, §§ 4, 4a BDSG; §§ 12, 13 TMG. Sie bezieht sich auf personenbezogene Daten, hinsichtlich derer die Beklagte von der Möglichkeit der Anonymisierung der Daten keinen Gebrauch macht. Die Klausel ist wie zuvor dargelegt eingebunden in die globale Einwilligung. Sie enthält keine inhaltliche Erklärung zu den konkreten Datenverarbeitungsprozessen und erweckt den - auch bei den vorherigen Klauseln beanstandeten - Eindruck einer wirksamen Einwilligung.

Klausel zu 8. (Weitergabe an Dritte) Die Klausel verstößt gegen § 307 Abs. 1 i. V. m. Abs. 2 Nr. 1 BGB, §§ 4, 4a BDSG; §§ 12, 13 TMG; §94 TKG. Die Klausel gibt keinen Aufschluss darüber, an welche konkreten Institutionen die Daten weitergegeben werden sollen. Sie geht damit eindeutig über den Bereich der Vertragserfüllung (§ 28 Abs. 1 Nr. 1 BDSG) hinaus. Sie bezieht sich auch auf Nutzungsdaten, beispielsweise des Telekommunikationsanbieters. Sie erlaubt insofern einen Datenaustausch und damit die Nutzung der Beklagten von Daten im Anwendungsbereich der §§ 91 ff. TKG. Nach § 94 Nr. 1 TKG muss die in diesem Zusammenhang erteilte Einwilligung jedoch „eindeutig" erteilt werden. Des Weiteren bedarf es einer Protokollierung.

Klausel zu 9. (Weitergabe an Dritte, Dienstleister) Diese Klausel verstößt gegen § 307 Abs. 1 i. V. m. Abs. 2 Nr. 1 BGB, §§ 4, 4a BDSG; §§ 12, 13 TMG; § 94 TKG; § 7 Abs. 2 UWG. Die vorliegende Klausel bezieht sich auf die Zwecke der Werbung, wie sich aus der Formulierung „Bewertung deines Interesses an unseren Produkten" ergibt. Die Regelung ermächtigt die Beklagte demzufolge, die personenbezogenen Daten des Kunden an Dritte weiterzugeben. Damit wird der Eindruck einer unwirksamen Einwilligung auch im Hinblick auf unerbetene Werbung erklärt, was zu einer unangemessenen Benachteiligung des Bestellers i, S. d. § 307 BGB führt.

Klausel zu 10. (Standortbezogene Dienste) Auch diese Klausel verstößt gegen § 307 Abs. 1 i. V. m. Abs. 2 Nr. 1 BGB; §§ 4, 4a BDSG; §§ 12, 13 TMG; § 94 TKG. Der Verbraucher erklärt mit dieser Regelung, dass Daten im Zusammenhang mit der Nutzung von Diensten der Beklagten „erhoben, genutzt und weitergegeben" werden. Trotz der zugesagten „Anonymisierung" ist - in dem für den Verbraucher ungünstigsten Fall - davon auszugehen, dass die Daten personenbeziehbar sein werden, da „standortbezogene Produkte und Dienste" angeboten werden sollen, was ohne eine hinreichende Individualisierung des angesprochenen Kunden nicht möglich wäre.

[Aus der Kostenentscheidung: D]ie mit einem Häkchen voreingestellte Formulierung „Am Ball bleiben - Haltet mich auf dem Laufenden mit den aktuellen Apple Infos. ..." verstieß gegen § 307 Abs. 1 i. V. m. Abs. 2 Nr. 1 BGB, § 7 Abs. 2 UWG. Denn der Verbraucher erklärt hiermit - möglicherweise ungewollt -die vorherige Einwilligung mit der Übermittlung unerwünschter Werbung. Auch der zweite Teil (Hinweis auf die Datenschutzvereinbarung) ist unzulässig, da hierdurch in Verbindung mit Ziff. 14 der AGB der Eindruck einer ausdrücklichen - nicht abdingbaren - Einwilligung erweckt wird. …

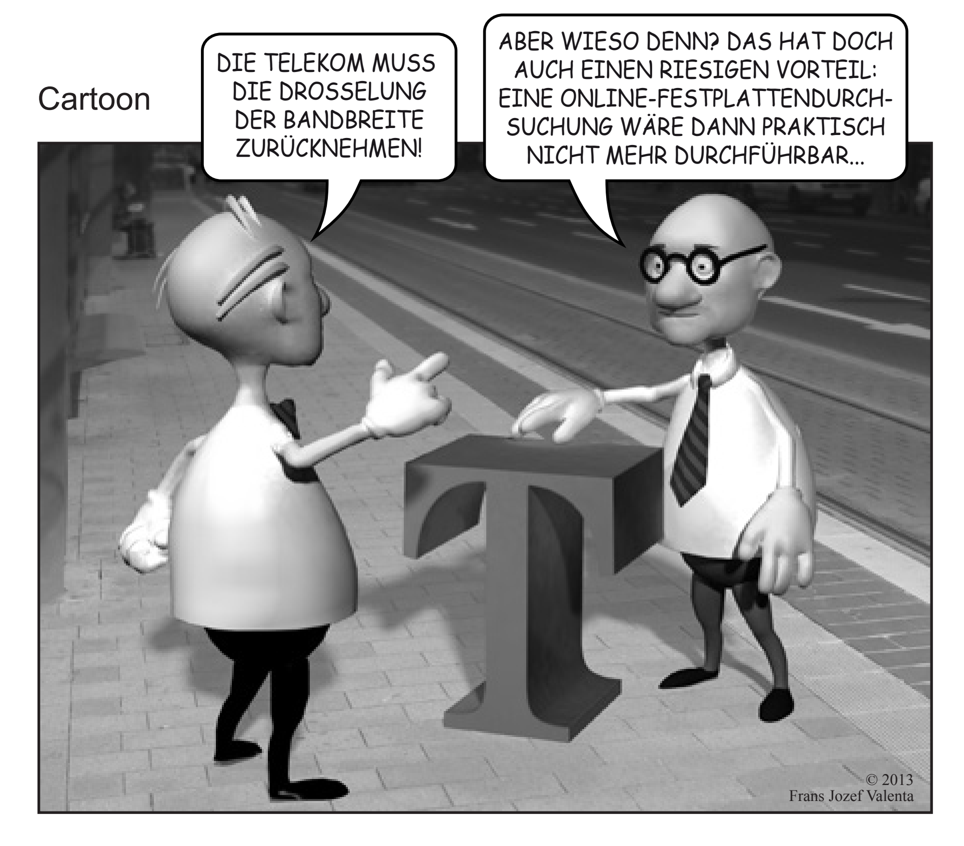
Siehe auch Seite 60 in diesem Heft.

LG Dresden

Massenhafte Funkzellenabfrage war unzulässig

Das Landgericht (LG) Dresden entschied mit Beschluss vom 17.04.2013, dass zwei Funkzellenabfragen um den

Cartoon



19.02.2011 im Bereich der Semperoper in Dresden rechtswidrig waren (Az. 15 Qs 34/12). Die hierbei erhobenen Daten sind wieder zu löschen. Die Abfrage einer anderen Funkzelle bewertete das Gericht für zulässig. Auf Antrag der Staatsanwaltschaft Dresden waren mehrere Dutzend Funkzellen abgefragt worden. Die Polizei hatte angegeben, mit der Aktion herausfinden zu wollen, ob Verdächtige, die in der Vergangenheit Polizisten angegriffen hatten, an der Demo teilnahmen. Wer sich in der Dresdner Südvorstadt aufhielt und ein eingeloggtes Mobiltelefon in der Tasche hatte, wurde so erfasst: Wer hatte wann mit wem telefoniert und sich dabei wo aufgehalten. Die Polizei erhob mehr als eine Million Datensätze und von mehr als 54.000 Mobilfunknutzern die sogenannten Stammdaten (Name, Adresse). Nach Presseberichten unter Berufung auf die Linke sollen bei der Gesamtaktion sogar mehr als eine Million Verkehrsdatensätze mit über 320.000 Rufnummern betroffen gewesen sein. Die Daten wurden auch bei Ermittlungen gegen Personen genutzt, die eine angemeldete Demonstration gestört haben sollen (DANA 3/2011, 119).

Das Amtsgericht (AG) Dresden hatte die Funkzellenabfrage zunächst genehmigt und anschließend die eigene Entscheidung für rechtens erklärt. Den Beschluss begründete das AG damit, dass Straftaten von erheblicher Bedeutung verfolgt wurden und daher die Abfragen erforderlich und angemessen gewesen seien. Das LG hob zwei der Beschlüsse vor allem aus formellen Gründen auf. In den Beschlüssen war kein Bezug zu schweren Gewalttätigkeiten hergestellt worden. Weitere Argumente gegen die Ermittlungsmaßnahme, insbesondere, dass unverhältnismäßig gegen eine viel zu unbestimmte Zahl von Personen vorgegangen wurde, wurden vom LG nicht anerkannt (Landgericht erklärt Funkzellenabfrage auf Demo für rechtswidrig, www.zeit.de 23.04.2013; Sachsen: Funkzellenabfrage bei Anti-Nazi-Protest war rechtswidrig, www.heise.de 25.04.2013; Volltextveröffentlichung: http://www.johannes-lichdi.de/fileadmin/user_upload/Judica/Handygate_LG_Dresden.pdf).

BayVGH

Automatisierte Kennzeichenerfassung zulässig

Gemäß einem Urteil des Bayerischen Verwaltungsgerichtshofes (BayVGH) in München vom 17.12.2012 ist die automatisierte Kennzeichenerfassung im Freistaat Bayern rechtlich nicht zu beanstanden (Az. 10 BV 09.2641). Allein die Erfassung der Autokennzeichen und ihr Abgleich mit polizeilichen Fahndungsdaten stelle noch keinen Eingriff in das Grundrecht auf informationelle Selbstbestimmung dar, soweit die Fahrzeugdaten danach sofort und spurenlos gelöscht werden (sog. „Nichttreffer“). Geklagt hatte ein Pendler, der auf seiner Strecke regelmäßig Geräte zur automatisierten Kennzeichenerkennung und -erfassung passiert. Mit seiner Klage wollte er erreichen, dass die Polizei Kennzeichen von auf ihn zugelassenen Fahrzeugen nicht mehr durch den verdeckten Einsatz automatisierter Kennzeichenerkennungssysteme erfasst und mit polizeilichen Dateien abgleicht. Es ging ihm darum, eine ständige polizeiliche Überwachung in der Art eines „Bewegungsbildes“ zu verhindern.

Gemäß dem Urteil des BayVGH hat das Verwaltungsgericht (VG) München die Klage zu Recht abgewiesen. Zwar liege ein konkreter Grundrechtseingriff in der nicht auszuschließenden fehlerhaften Erfassung der Kennzeichen (sog. „unechter Treffer“), weil in diesem Fall eine Nachkontrolle durch einen Polizeibeamten erfolge. Dieser Eingriff sei aber gerechtfertigt. Die Vorschriften, die die automatisierte Kennzeichenerfassung ermöglichen, seien verfassungsgemäß. Der bayerische Gesetzgeber sei zu der den Kläger betreffenden Regelung zuständig, weil sie im Ergebnis rein präventiven Charakter habe. Die Frage der Gesetzgebungskompetenz für eine Regelung zur weiteren Verwendung der durch die Kennzeichenerfassung erhobenen Daten, evtl. auch im Rahmen strafverfolgender Tätigkeit sei nicht Gegenstand des entschiedenen Falls. Die einschlägigen Vorschriften des Polizeiaufgabengesetzes (PAG) seien hinreichend bestimmt, die Löschung der erhobenen Daten klar geregelt. Das verfassungsrechtliche Gebot der Verhältnismäßigkeit werde noch gewahrt. Der Gesetzgeber habe schwerwiegende Eingriffe, die nur zu besonders gewichtigen Zwecken erfolgen dürften, von vornherein ausgeschlossen oder eng begrenzt. So sei es nur in besonderen Fällen zulässig, Einzelerfassungen zu einem Bewegungsbild zu verbinden. Der flächendeckende Einsatz der Kennzeichenerfassung sei grundsätzlich nicht erlaubt. Da die Kennzeichenerfassung und der Datenabgleich nicht anlasslos und nur bei Vorliegen bestimmter Gefahrenlagen erfolgten, werde keine unbegrenzte Kontrolle aller Verkehrsteilnehmer ausgeübt. Auch ein rechtswidriger Vollzug der gesetzlichen Bestimmungen liege derzeit in Bayern nicht vor (Bayerischer Verwaltungsgerichtshof erklärt automatisierte Kennzeichenerfassung für zulässig; http://www.kostenlose-urteile.de 15.03.2013; Gericht erlaubt Nummern-Kontrolle, SZ 16./17.03.2013, 47).

VG Freiburg

Dauerobservation von früherem Sexualstraftäter gestoppt

Das Verwaltungsgericht (VG) Freiburg untersagte der Polizeidirektion Freiburg mit Urteil vom 14.02.2013, die Observation eines mehrfach verurteilten Sexualstraftäters weiter fortzuführen (Az. 4 K 1115/12). Für die jahrelange Observation als rückfallgefährdet angesehener Sexualstraftäter zum Zwecke der Verhinderung erneuter Sexualstraftaten fehlt es in Baden-Württemberg derzeit an einer Rechtsgrundlage. Der Kläger des zugrunde liegenden Streitfalls war im September 2010 aufgrund eines Urteils des Europäischen Gerichtshofs für Menschenrechte (EGMR) aus der Sicherungsverwahrung entlassen worden. Dort hatte er sich zwanzig Jahre lang - davon zehn Jahre zu Unrecht - befunden, weil er in der Zeit von 1976 bis 1985 Vergewaltigungen begangen hatte, dafür mehrfach verurteilt und seit Verbüßung seiner letzten Haftstrafe als rückfallgefährdet eingeschätzt worden war. Seit der Entlassung aus der Sicherungsverwahrung waren ihm in den letz-

ten zwei Jahren außerhalb seiner Wohnung Zivilbeamte auf Schritt und Tritt überall hin gefolgt, um so womöglich erneuten Sexualstraftaten vorzubeugen.

Das VG Freiburg führte aus, dass diese insgesamt 17 mal vom Leiter der Polizeidirektion Freiburg für jeweils mehrere Wochen angeordnete Dauerobservation einen schweren Grundrechtseingriff darstelle. Auch einem Mehrfach-Sexualstraftäter stehe ein Recht auf einen Bereich autonomer privater Lebensgestaltung außerhalb seiner häuslich privaten Sphäre zu. Für einen solchen Eingriff in das Persönlichkeitsrecht bedürfe es einer speziellen und ausdrücklichen gesetzlichen Grundlage. Diese fehle hier.

Die Vorschrift im Landespolizeigesetz (PolG), die „als besonderes Mittel der Datenerhebung" eine - ohnehin nur zeitlich begrenzte - Observation zum Zwecke der Sammlung personenbezogener Daten des Observierten zulasse, tauge nicht als Rechtsgrundlage für die jahrelange Dauerüberwachung. Denn im vorliegenden Fall gehe es nicht um die Gewinnung von Erkenntnissen über die persönlichen oder sachlichen Verhältnisse oder um die Herstellung von Bewegungsprofilen des der Polizei ja bereits wohlbekannten Klägers. Vielmehr diene die völlig offene Überwachung in Form seiner dauernden Begleitung durch Zivilbeamte allein der Abwehr von ihm womöglich ausgehender Übergriffe. Dafür sei die gesetzliche Regelung aber nicht geschaffen worden. Bereits der Verwaltungsgerichtshof Baden-Württemberg habe im Herbst 2011 Zweifel an der Tauglichkeit dieser Vorschrift als Rechtsgrundlage für eine jahrelange Dauerüberwachung geäußert. Trotzdem habe der Gesetzgeber bis heute keine neue spezielle Gesetzesgrundlage geschaffen. Die Vorschrift könne deshalb nicht - auch nicht mehr übergangsweise - als noch ausreichende Rechtsgrundlage herangezogen werden.

Das gelte auch für die Bestimmung im PolG, welche die Polizei ganz pauschal ermächtige, zur „Abwehr von Gefahren für die öffentliche Sicherheit" die „nach ihrem Ermessen erforderlichen" Maßnahmen zu treffen. Auf diese Vorschrift lasse sich die langjährige Observation jedenfalls heute nicht einmal mehr übergangsweise stützen. Der demokratisch legitimierte Gesetzgeber dürfe nämlich wesentliche Entscheidungen nicht der Verwaltung als vollziehender Gewalt überlassen. Vielmehr sei er gehalten, für intensive, besondere polizeiliche Eingriffe deren Anlass, Zweck und Grenzen selbst hinreichend klar und bestimmt durch eine spezifische gesetzliche Ermächtigungsvorschrift ausdrücklich festzulegen. Das habe der Gesetzgeber aber bisher trotz ausreichend langer Übergangszeit nicht getan.

Das VG führte außerdem aus, dass die Observation nicht nur mangels gesetzlicher Grundlage rechtswidrig sei. Selbst wenn die genannten Vorschriften bis zu einer speziellen Regelung der Materie durch den Gesetzgeber noch übergangsweise als Grundlage akzeptiert würden, fehle es im konkreten Fall an einer vom Kläger für Dritte noch ausgehenden aktuellen und konkreten Gefahr. Zu dieser Einschätzung kam das Gericht aufgrund der in der fünfstündigen mündlichen Verhandlung durchgeführten ausführlichen Anhörung des Klägers selbst, seines Bewährungshelfers, des behandelnden Psychotherapeuten und der ihn überwachenden Polizeibeamten. Das letzte Gutachten, das dem Kläger noch eine gewisse Rückfallgefährdung attestiere, stamme noch aus der Zeit der Sicherungsverwahrung. Nach der Rechtsprechung des Bundesverfassungsgerichts müsse eine aktuelle Prognose aber auf der Basis des Verhaltens in Freiheit angestellt werden. Insoweit aber ergebe sich eine Gefährdung entgegen der Ansicht der Polizei nicht schon daraus, dass der Kläger nicht ausreichend mit den ihn überwachenden Polizisten kooperiere. Denn dazu sei er rechtlich nicht verpflichtet. Der Kläger sei seit der Erledigung der Sicherungsverwahrung im Jahr 2010 ein freier Mann, der die Weisungen der Führungsaufsicht einzuhalten habe, was er auch tue, der sich aber im Übrigen ebenso verhalten könne wie jeder andere freie Mensch. Der Kläger sei insbesondere nicht verpflichtet, seine Aktivitäten, insbesondere Fahrradtouren, den observierenden Polizeibeamten vorher ankündigen. Für das Gelingen der Observation müsse er nicht Sorge tragen. Unkooperatives Verhalten in diesem Zusammenhang könne ihm daher nicht vorgeworfen werden. Der Kläger nehme im Übrigen regelmäßig und pünktlich, ohne dass er dazu verpflichtet sei, an einer wöchentlichen Psychotherapie teil und habe nach Aussagen des Therapeuten nachvollziehbar Fortschritte gemacht. Der Bewährungshelfer schätze wie auch der behandelnde Psychologe das Risiko als sehr gering ein. Da es keine Anhaltspunkte für eine Gefährlichkeit des Klägers gebe, sei die Dauerüberwachung einzustellen (Keine polizeiliche Dauerobservation eines früheren Sexualstraftäters, www.kostenlose-urteile.de 22.03.2013).

BAG

Arbeitgeber darf Datenschutz bei Betriebsrat nicht kontrollieren

Das Bundesarbeitsgericht (BAG) entschied mit Beschluss vom 18.07.2012, dass der Arbeitgeber dem Betriebsrat keine Vorschriften zur Einhaltung des Bundesdatenschutzgesetzes (BDSG) machen darf (Az.: 7 ABR 23/11). Der Betriebsrat eines Einzelhandelsunternehmens hatte einen Sammelaccount gefordert, bei dessen Nutzung sich das einzelne Betriebsratsmitglied nicht unter seinem Namen anmelden muss. Der Arbeitgeber lehnte dies aus Gründen des Datenschutzes ab. Er wolle gemäß § 9 Satz 1 BDSG und dessen Anlage nachverfolgen, wer auf den Rechner zugreift, um so eine möglichst effektive Eingabekontrolle zu haben. Das BAG entschied jedoch, dass der Arbeitgeber dem Betriebsrat beim Datenschutz keine Vorschriften machen dürfe. Die Arbeitnehmervertreter könnten vom Arbeitgeber die Einrichtung eines Gruppenaccounts verlangen, der es dem Unternehmen nicht ermöglicht, die Internetnutzung durch die einzelnen Betriebsratsmitglieder nachzuvollziehen. Das BDSG schreibe zwar für den Rechner des Betriebsrats datenschutzrechtliche Sicherungen vor. Für entsprechende Maßnahmen müsse der Betriebsrat jedoch in eigener Verantwortung sorgen. Er habe daher auch eigenständig darüber zu beschließen, wie er den Anforderungen des Datenschutzes Rechnung trägt.

Aus der Entscheidung ergibt sich indirekt, dass der Betriebsrat auch selbst darüber entscheidet, welche Beschäftig-

tendaten er zur Erfüllung seiner Aufgaben erhebt und verwendet. In einer anderen Entscheidung zum Umfang des Kontrollrechts des Betrieblichen Datenschutzbeauftragten (DSB) hatte das Gericht entschieden, dass dieser den Betriebsrat nicht daraufhin kontrollieren darf (oder muss), ob er die Vorschriften zum Datenschutz beachtet. Schließlich würde der Datenschutzbeauftragte vom Arbeitgeber ausgesucht (Wybitul, Welche Daten über mich darf der Arbeitgeber verlangen? www.faz.net, 10.02.2013; juris.bundesarbeitsgericht.de).

VG Wiesbaden

Verwertungsverbot für unzulässig gespeicherte Daten

Am Beispiel der von dem Bundeskriminalamt geführten Datei „Visa-KzB-Verfahren" zeigt das VG Wiesbaden in dem Urteil vom 04.04.2013 - Gesch.Z.: 6 K 910/12.WI.A - dass Daten aus Dateien, welche ohne hinreichende Rechtsgrundlage und unter Verstoß gegen formelles Datenschutzrecht errichtet wurden, auch einer richterlichen Entscheidungsfindung nicht zu Grunde liegen dürfen. Wie dokumentieren Auszüge dieser Entscheidung:

Leitsätze:

1. Die INPOL-A-Datei „Visa-KzB-Verfahren" ist rechtswidrig.

2. Die Art der Daten, die in polizeilichen Informationssystemen des BKA gespeichert werden dürfen, sind durch Rechtsverordnung zu regeln.

3. Die Verarbeitung von Visa-Daten erfolgt nach allgemeinen datenschutzrechtlichen Grundsätzen, dies mit der Folge, dass eine Meldung vorliegen und eine Vorabkontrolle durch den behördlichen Datenschutzbeauftragten erfolgen muss.

4. Sind Daten rechtswidrig gespeichert, so sind sie zu löschen.

5. Rechtswidrig gespeicherte Daten unterliegen einem Verwertungsverbot.

[Aus der Entscheidungsbegründung:] Der Kläger … meldete sich am 23.05.2012 bei der Erstaufnahmeeinrichtung … und wurde am selben Tag vom Bundesamt für Migration und Flüchtlinge erkennungsdienstlich behandelt. … Zu seiner Einreise machte er bei seiner Anhörung keinerlei Angaben. … Mit Bescheid des Bundesamtes für Migration und Flüchtlinge vom 20.07.2012 wurde festgestellt, dass die Voraussetzungen für die Zuerkennung der Flüchtlingseigenschaft und Abschiebeverbote nach § 60 Abs. 2 – 7 AufenthG nicht vorliegen. … Zur Begründung wurde im Wesentlichen ausgeführt, dass die Glaubhaftigkeit des Klägers bereits deshalb erheblich gemindert sei, weil bereits die Glaubhaftigkeit seiner Fluchtschilderung wegen seiner Weigerung, den Reiseweg zu schildern, nicht gegeben sei. … Die Beklagte .. legt im Weiteren Asylverfahren einen Auszug aus der Datei „Visa-KzB-Verfahren" des Bundeskriminalamtes (BKA) vor, aus dem sich ergibt, dass dem Kläger von der ___ Botschaft in ___ ein Visum … ausgestellt worden war. Aus der legalen Ausreise ergebe sich, dass keine Verfolgungsabsicht des ___ Staates vorliege. Durch das Vorenthalten von Informationen zu den näheren Umständen der Ausreise, welche eben auch Informationen über die Notwendigkeit der Flucht und damit des Verfolgungsgeschehens mit sich führten, habe der Kläger in einer bedenklichen und erklärungsbedürftigen Weise die Rezeption seines Sachvortrags gesteuert und nachträglich gerade manipuliert.

Die zulässige Klage ist begründet. … Soweit die Beklagte unter Vorlage aus dem Ausdruck der Datei Visa-KzB-Verfahren und den daraus beruhenden Erkenntnissen die Unglaubwürdigkeit des Vortrages des Klägers zu begründen versucht, unterliegen diese Informationen einem Verwertungsverbot. Denn die INPOL-A-Datei „Visa-KzB-Verfahren" ist rechtswidrig, soweit diese Datei ihre Rechtsgrundlage in § 7 BKA-Gesetz hat. … Insoweit regelt § 7 Abs. 1 BKA-Gesetz, dass das BKA personenbezogene Daten speichern, verändern und nutzen kann, soweit dies zur Erfüllung seiner jeweiligen Aufgaben als Zentralstelle erforderlich ist. Soweit das BKA Dateien als Zentralstelle im polizeilichen Informationssystem nach § 11 BKA-Gesetz führt, sind gemäß § 7 Abs. 6 BKA-Gesetz durch Rechtsverordnung des Bundesministeriums des Innern, welche mit Zustimmung des Bundesrates zu ergehen hat, dass Nähere über die Art der Daten, die gespeichert werden dürfen, zu regeln … Die Verordnung über die Art der Daten, die nach §§ 8 und 9 BKAG gespeichert werden dürfen, regelt mithin sämtliche Daten, die im polizeilichen Informationssystem gespeichert werden dürfen. Die Verordnung enthält jedoch nicht die Daten, welche im Visa-KzB-Verfahren ebenfalls erforderlich sind, wie z. B. Einreisedatum, Ausreisedatum, gewünschte Aufenthaltsdauer, Zweck des Aufenthalts, FIS-Aktenzeichen, privilegierter Familienangehöriger eines EU-Bürgers, usw.. Damit fehlt es bereits an der erforderlichen Bestimmung der Art der Daten, die nach §§ 8 und 9 BKA-gespeichert werden dürfen, dies mit der Folge, dass die Datenspeicherung beim BKA rechtswidrig ist (vgl. VG Gießen, Urteil vom 29.04.2002, Az. 10 E 141/01 - nach Juris, OVG Lüneburg, Urteil vom 16.12.2008, Az. 11 LC 229/08 - nach Juris).

Soweit sich das BKA als Ermächtigung zur Datenspeicherung auch auf § 73 Abs. 3 Satz 3 AufenthG und Art. 22 und 31 Visa-Kodex beruft, ändert dies an der rechtswidrigen Speicherung der Daten nichts. § 73 Abs. 3 Satz 3 AufenthG regelt lediglich, dass die in Satz 1 genannten Behörden (u. a. BKA) die übermittelten Daten speichern und nutzen dürfen, soweit dies zur Erfüllung ihrer gesetzlichen Aufgaben erforderlich ist. Dies bedeutet jedoch keine Ermächtigung zu einer Speicherung in einem polizeilichen Informationssystem. Insoweit liegt ein Verstoß gegen die bereichsspezifischen Regelungen des BKA-Gesetzes vor.

Auch sind die Regelungen aus der Verordnung (EG) Nr. 810/2009 des Europäischen Parlaments und des Rates vom 13.07.2009 über einen Visa-Kodex der Gemeinschaft (Visa-Kodex) (Abl. L 234 v. 15.09.2009) zuletzt geändert durch Verordnung Nr. 153/2012 vom 15.02.2012 (L 58, S. 3) keine Rechtsgrundlage zu einer Speicherung in einem polizeilichen Informationssystem.

Vielmehr ergibt sich aus Art. 22 Visa-Kodex VO lediglich, dass zentrale Behörden eines Mitgliedstaates bei der Prüfung der Staatsangehörigen von spezifischen Drittländern zu konsultieren sind für Frage, ob Einwände gegen ein Visum bestehen bzw. gem. Art. 31 ein Mitgliedstaat verlangen kann, dass seine zentrale Behörde von den Konsulaten anderer Mitgliedstaaten entsprechend informiert werden. Damit ist lediglich eine Rechtsgrundlage zur Übermittlung der Daten zum Zwecke der entsprechenden Entscheidung, vorliegend Visa-Erteilung „ja“ oder „nein“, von anderen europäischen Staaten an zentrale Behörden - hier das BKA - geregelt. Nicht jedoch, wie die zentralen Behörden mit den Daten nach dieser Entscheidung weiter umzugehen haben.

Vielmehr ergibt sich aus Erwägungsgrund 12 der Verordnung Nr. 810/2009, dass für personenbezogene Daten, die von den Mitgliedstaaten in Anwendung dieser Verordnung verarbeitet werden, die Richtlinie 95/46 EG des Europäischen Parlaments und des Rates vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (EG-Datenschutzrichtlinie, ABl. L 281 vom 23.11.1995, S. 31) Anwendung findet. Dies bedeutet insoweit, dass Art. 3 Abs. 2 EG-Datenschutzrichtlinie, welcher sich auf die öffentliche Sicherheit und Strafverfolgung bezieht, vorliegend gerade keine Anwendung findet.

Mithin hätte das BKA, soweit es die Visa-Daten weiterhin speichern will, die Datenspeicherung nach allgemeinen datenschutzrechtlichen Grundsätzen (Erforderlichkeit und Zweckbindung, vgl. § 14 BDSG) durchführen müssen, mit der Folge, dass die Datei nicht als Zentraldatei im Rahmen eines polizeilichen Informationssystems, sondern als allgemeine Datei zu führen wäre und damit einer Meldung nach Art. 18 EG-Datenschutzrichtlinie unterliegt. Dies mit der Folge, dass eine Meldung gemäß § 4 e BDSG zum Zeitpunkt der Verarbeitung hätte vorliegen müssen (vgl. EuGH, Urteil vom 09.11.2010, Az. C-92/09 u.a., Rdnr. 101).

Auch hätte es eine Vorabkontrolle durch den behördlichen Datenschutzbeauftragten des BKA gemäß § 4 d Abs. 5 und 6 BDSG bedurft, da die Daten gerade dazu bestimmt sind, die Persönlichkeit des Betroffenen zu bewerten (Visa-Erteilung: ja oder nein). Eine entsprechende Meldung liegt ebensowenig vor, wie eine Vorabkontrolle durch den behördlichen Datenschutzbeauftragten des BKA.

Damit ist eine Datenspeicherung unzulässig und die Daten sind zu löschen (§ 32 Abs. 2 Satz 1 BKA-Gesetz = § 20 Abs. 2 Nr. 1 BDSG).

Damit ist eine Übermittlung nach polizeirechtlichen Grundsätzen nicht möglich. Gemäß Art. 6 Abs. 1 Ziff. c EG-Datenschutzrichtlinie haben die Mitgliedstaaten vorzusehen, dass die personenbezogenen Daten den Zwecken entsprechend für diese erhoben oder weiterverarbeitet werden, dafür erheblich sind und nicht darüber hinausgehen. Der Zweck der übermittelten Daten ist durch den Visa-Kodex festgelegt. Gemäß Art. 22 Abs. 2 Visa-Kodex VO haben die konsultierten zentralen Behörden das Ersuchen auf jeden Fall innerhalb von sieben Kalendertagen nach dem Eingang zu beantworten, andernfalls bedeutet dies, dass keine Einwände für die Erteilung eines Visums bestehen. Anschließend entfällt der weitere Zweck der Daten. Eine Zweckänderung sieht der Visa-Kodex nicht vor.

Soweit die Bundesrepublik Deutschland eine Zweckänderung über den Visa-Kodex hinaus vorsehen wollte, wäre dies – soweit europarechtlich zulässig – spezialgesetzlich zu regeln. Hierzu reicht § 73 Abs. 3 Satz 3 AufenthG nicht aus, wenn ausgeführt wird, dass die übermittelten Daten für eigene Zwecke gespeichert und genutzt werden dürfen, hingegen Übermittlungsregelungen nach anderen Gesetzen unberührt bleibt. Damit wird der Bestimmtheitsgrundsatz von Art. 6 EG-Datenschutzrichtlinie durchbrochen (siehe insoweit zur unmittelbaren Wirkung der Richtlinie - hier Art. 7 Buchstabe f EG-Datenschutzrichtlinie - EuGH, Urteil vom 24.11.2011, Az. C-468/10 u.a.).

Nach alledem durften die in das Verfahren eingeführt Daten durch die Beklagte vom Bundeskriminalamt nicht mehr gespeichert sein. Dies mit der Folge, dass das Bundeskriminalamt diese auch nicht hätte weitergeben (also übermitteln) dürfen.

Gemäß § 32 Abs. 2 Satz 1 BKA-Gesetz (entspricht § 20 Abs. 2 Ziff. 1 BDSG), sind personenbezogene Daten, die automatisiert verarbeitet werden, zu löschen, wenn ihre Speicherung unzulässig ist. Gemäß § 32 Abs. 6 BKA-Gesetz (entspricht § 20 Abs. 8 BDSG) sind die Stellen zu verständigen, denen im Rahmen einer Übermittlung die Daten zur Speicherung weitergegeben wurden, wenn die Daten zu löschen sind. Dies dient der Sicherstellung der Zweckbindung und führt zu einem Verwertungsverbot bei allen speichernden Stellen.

[Es folgen die Entscheidung ebenfalls tragende Erwägungen zum Fluchtschicksal des Klägers.]

Thilo Weichert

Wilhelm Steinmüller ist tot

Prof. Dr. Wilhelm Steinmüller ist am 1. Februar 2013 im Alter von 78 Jahren gestorben. Steinmüller war ein Pionier des deutschen Datenschutzes und zugleich viel mehr: Er wurde in Ludwigshafen geboren und wuchs in München auf. Er studierte Jura, Theologie, Philosophie und Volkswirtschaft. Er war immer auf Entdeckungstour. Hatte er eine Entdeckungsreise abgeschlossen, so widmete er sich neuen Ufern. Er blieb ein Theoretiker und Wissenschaftler, den die Praxis eher als Feld für Studien, des Diskurses und der Aufklärung interessierte und weniger als Feld zur Weltverbesserung. Auch wenn er zeitlich in die 68er passte, so war er nie einer von ihnen. Gemeinsam hatte er mit den 68ern seine Beschäftigung mit der Nazizeit und die Notwendigkeit des Widerstands gegen totalitäre Fremdbestimmung.

Es gab zwei große Wechsel in seinem Leben: Ende der 60er Jahre wandte er sich von der Rechtstheologie ab – er hatte einen Lehrstuhl für Kirchenrecht in Regensburg – und kümmerte sich plötzlich um das von ihm mitbegründete Fach der Rechtsinformatik. Einer seiner Assistenten in Regensburg, Hansjürgen Garstka, war dann einer, der als Berliner Datenschutzbeauftragter die Entwicklung des Datenschutzrechtes von Anfang an stark mitbestimmte. Die zweite Zäsur vom „Lehrer" zum „Helfer" fand Ende der 80er/Anfang der 90er Jahre statt, als er sich von der Informatik abwandte und seitdem als Psychotherapeut tätig war, zunächst in den USA, wo seine Entdeckungsreise ihn auch zur Zentherapie oder zu schamanischen und tantrischen LehrerInnen führte. Eine seiner Schwerpunktaktivitäten als Psychotherapeut war die Trauma-Aufarbeitung. Diese Ausbildung ermöglichte es ihm, die sicherheitspolitischen datenschutzkritischen Aktivitäten der Innenminister Schily und Schäuble zu Beginn des neuen Jahrtausends aus einem ungewöhnlichen Blickwinkel zu betrachten.

Der Schwerpunkt eines Nachrufes muss bei Steinmüller beim Datenschutz liegen, wobei er diesen nie verengt als Privatsphärenschutz verstand, sondern – als Ergebnis einer systemtheoretischen Analyse – als informationelle Selbstbestimmung. Dieser Begriff, der später vom Bundesverfassungsgericht anlässlich der Volkszählungsentscheidung 1983 zum Grundrecht erhoben wurde, wurde von ihm – gemeinsam mit einigen jungen Wissenschaftlern um ihn herum, darunter Bernd Lutterbeck – erstmals verwendet in dem 1971 für das Bundesministerium des Innern erstellten Gutachten „Grundfragen des Datenschutzes" vom Juli 1971, das aber erst 1983 veröffentlicht wurde (BT-Drs. VI/3826). Er sah nicht in den Daten die Gefahr für die Menschen, sondern in der Nutzung dieser Daten, die Macht und Geld versprechen. Intellektuell herausgefordert war er von den – damals in vieler Hinsicht unrealistischen – Visionen von Technikanbietern wie IBM und Siemens oder administrativen Technokraten wie dem damaligen Präsidenten des Bundeskriminalamtes Horst Herold, die die unbegrenzte Verfügbarkeit der Daten und deren Verwendung propagierten. Sein Reflex darauf war die – technisch realisierbare und rechtlich zu erzwingende – „Datenzuteilung". Als Zweckbindungsprinzip wurde diese 1983 vom Bundesverfassungsgericht verfassungsrechtlich zur Norm erhoben. Wie aktuell sein Ansatz heute ist, zeigen die Big-Data-Visionen, die inzwischen technisch erheblich realistischer sind als vor 40 Jahren. In den USA ist der Zweckbindungsgrundsatz bis heute noch nicht anerkannt.

Steinmüller erkannte und erlebte die Diskussion um den Datenschutz als einen Kampf um die Verfügungsmacht über Daten. In diesem Kampf gab und gibt es zwei Gruppen von Bedarfsträgern, die sich mit mehr oder weniger lauteren Mitteln diese Macht aneignen wollen: die Verwaltung und die Wirtschaft. Während die Verwaltung die Macht des Faktischen für sich hatte, die mit dem Volkszählungsurteil grundrechtlich gezähmt wurde, nutzte die Wirtschaft die Macht der Lobby. Anfang der 70er Jahre war das vorrangig die Lobby der Adresshändler und der Mediziner. Inzwischen sind viele weitere Lobbyisten dazugekommen. Steinmüller war kein Straßenkämpfer; diese Rolle überließ er anderen – der außerparlamentarischen Opposition, z. B. den VolkszählungsgegnerInnen, für die er aber einen theoretischen Hintergrund herstellte und die er etwa in einem Institut für Kommunikationsökologie (IKÖ) in Bremen unterstützte. Auch war er nicht der strategisch politisch Handelnde, selbst wenn er als Gutachter in den Parlamenten herumgereicht wurde; diese Rolle nahmen die Datenschutzbeauftragten wahr mit Spiros Simitis an der Spitze. Seine Welt blieb

die der Wissenschaft und der Theorie, wobei er sich insofern – anders als sein Freund und Lehrer Adalbert Podlech – auch mit provokanten Diskussionsbeiträgen zu Wort meldete.

Wilhelm Steinmüller verstand sich als Kommunikator; dabei hatte er Ecken und Kanten. Sein Anliegen war es, in der Informatikära eine vermittelnde Sprache zwischen Gesellschaft, Recht und Technik zu finden. Hierfür schrieb er ein dickes Buch als Vermächtnis: „Informationstechnologie und Gesellschaft – Einführung in die Angewandte Informatik“ (Darmstadt, 1993, abrufbar unter http://www.informaticsapplied-textbook.info/). Die Bezeichnung „Einführung“ ist ein Euphemismus; weniger bescheiden nannte er es auch das „weltweit erste und bisher umfassendste Lehrbuch für angewandte Informatik“. Es handelt sich eigentlich um fünf Bücher mit insgesamt 745 Seiten, in denen Steinmüller eine Theorie der Informationsgesellschaft – im wahrsten Sinne des Wortes „zusammenbaute“. In seinen Zettelkästen hatte er die Informationen gesammelt, aus denen er Bauplan, Baumaterial, Gebäude, Umwelt und Baukunst schuf. Das Werk, bei dem „informationelle Selbstbestimmung“ nur ein Aspekt unter vielen ist, wurde kaum rezipiert; die technische Entwicklung des Internet war rasant; für eine soziologische oder gesellschaftskritische Hinterfragung bestand keine nennenswerte Nachfrage. Für Steinmüller blieb das Internet ein „riesiger Computer mit zu viel Drähten.“ Alles ist vernetzt; alles wird überwacht. Er blieb die ganze Zeit seiner Informatikära ein Nichttechniker. Dies waren Gründe genug für Steinmüller, seine zweite Zäsur im Leben zu vollziehen – die vom Informatiker zum Psychotherapeuten. Die letzten Jahre seines Lebens seit 2006 verbrachte er in Berlin. Dort besuchten ihn zwei Mitarbeiter des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein, Martin Rost und Henry Krasemann, und führten mit ihm ein einstündiges Interview, das im Internet abrufbar ist und die Erinnerung wachhält an einen eigenwilligen Pionier des Datenschutzes, dessen grundlegende Anliegen von bürgerrechtlich motivierten Datenschützern weiter verfolgt werden und verfolgt werden müssen (https://www.datenschutzzentrum.de/interviews/steinmueller/).




DATENSCHUTZ HAT BEI UNS EINEN SEHR HOHEN STELLENWERT. WIR MÖCHTEN SCHLIESSLICH NICHT, DASS EIN WHISTLEBLOWER LEAKT, WELCHE IHRER DATEN WIR MIT PRISM AUSSPÄHEN.